DATED

THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION

and

PEARSON EDUCATION LIMITED

CONTRACT FOR THE PROVISION OF SERVICES IN RELATION TO THE DIGITAL: DIGITAL SUPPORT SERVICES T LEVEL TECHNICAL QUALIFICATION

Contents

1 Contract start, formation and interpretation 5

2 Appointment and exclusivity 6

3 How the Services must be supplied 7

4 Pricing and payments 9

5 Developing the TQ and achieving IfATE Approval 12

6 Operating the TQ 19

7 Interaction with Providers 20

8 TQ Changes 22

9 Record keeping, monitoring and reporting 25

10 Staff Transfer 26

11 Supplier Staff and Subcontracting 27

12 Rights and protection 27

13 Intellectual Property Rights 29

14 What may happen if there are issues with your provision of the Services 34

15 Ending or extending this Contract 38

16 How much each Party can be held responsible for 41

17 Insurance 42

18 Data protection and information 43

19 What must be kept confidential 45

20 When information can be shared 47

21 Invalid parts of this Contract 48

22 No other terms apply 48

23 Other people's rights in this Contract 49

24 Circumstances beyond either Party's control 49

25 Relationships created by this Contract 49

26 Giving up contract rights 50

27 Transferring responsibilities 50
28 Changing this Contract 50
29 How to communicate about this Contract 52
30 Dealing with claims 53
31 Preventing fraud, bribery and corruption 54
32 Equality, diversity, human rights and modernslavery 55
33 Health and safety 56
34 Environment 56
35 Tax 56
36 Conflict of interest 57
37 Reporting a breach of this Contract 57
38 Resolving disputes 57
39 Which law applies 58
Schedule 1 - Definitions and Interpretation 60
Schedule 2 - Service Requirements 99
Schedule 3 - Implementation 500
Schedule 4 - Co-operation 544
Schedule 5 - Supplier's Response 548
Schedule 6 - Pricing Schedule 653
Schedule 6A - Adaptive Pricing 663
Schedule 7 - Staff (including Key Personnel) 667
Schedule 8 - Supply Chain (including approved Subcontractors) 673
Schedule 9 - Data Handling and Security Management 676
Schedule 10 - Business Continuity 681
Schedule 11 - Change Management 688
Schedule 12 - Exit Management 689
Schedule 13 - Form of Guarantee 799
Schedule 14 - Form of Assignment and Licence 800

Schedule 15 - Monitoring of Performance 825
Schedule 16 - Logos and Trademarks – T Level Trade Mark Licence 841
Schedule 17 - Provider Contract requirements 875
Schedule 18 - Commercially Sensitive Information 879
Schedule 19 - Required Insurances 882
Schedule 20 - Authorised Representatives 885
Schedule 21 - Staff Transfer 887

THIS CONTRACT is made on

BETWEEN:

(1) **THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION** of Sanctuary Buildings, 20 Great Smith Street, London SW1P 3BT ("**Authority**"); and

(2) **PEARSON EDUCATION LIMITED**, a company registered in England and Wales (company registration number: **00872828**), whose registered office is at **Hailey Court, Jordan Hill Business Park, Oxford, OX2 8EJ** ("**Supplier**"),

each a "**Party**" and together the "**Parties**".

BACKGROUND TO THIS CONTRACT:

(A) On **3rd December 2023** the Authority advertised in the Find a Tender Service (FTS) (reference **2023/S 000-035661**) inviting prospective suppliers to submit proposals for the design development and delivery of the technical education qualification element for the **Digital Support Services** T Level.

(B) On the basis of the Supplier's response to the advertisement and a subsequent tender process, the Authority selected the Supplier as its preferred supplier of the TQ.

(C) The Parties have agreed to contract with each other in accordance with the terms and conditions set out below. As well as the delivery stage, this Contract covers the Development Phase and a Pre-Delivery Phase.

OPERATIVE TERMS:

1 Contract start, formation and interpretation

1.1 This Contract is legally binding from the Effective Date until it ends in accordance with clause 15 (*Ending or extending this Contract*).

1.2 This Contract is formed by the Core Terms and the Schedules and the Supplier must comply with all of its obligations set out in both the Core Terms and the Schedules, provided always that in the event of any conflict between the provisions of the Core Terms and the Schedules and/or the Annexes, or between any of the Schedules and/or the Annexes, the conflict shall be resolved according to the following descending order of priority:

1.2.1 the Core Terms, Schedule 1 (*Definitions and Interpretation*), and Schedule 6 (*Pricing Schedule*);

1.2.2 Schedule 2 (*Service Requirements*), Schedule 4 (*Co-operation*) and their respective Annexes; and

1.2.3 the remaining Schedules and their respective Annexes.

1.3 The Parties shall interpret this Contract using Schedule 1 (*Definitions and Interpretation*).

2 Appointment and exclusivity

2.1 The Authority hereby appoints the Supplier as the provider of the Services in relation to the TQ during the Term.

2.2 As part of such appointment, the Supplier has the exclusive right to offer the TQ in England to Students for TQ courses for the Cohort for the Academic Years commencing at each of 1 August 2025, 1 August 2026, 1 August 2027, 1 August 2028, 1 August 2029 and, where the Authority gives written notice to the Supplier to extend this Contract pursuant to clause 15.2 (*Ending or extending this Contract*), for each of the Cohorts for the Academic Years commencing during an Extension Period, as the case may be, namely 1 August 2030, 1 August 2031, 1 August 2032 (each an "**Exclusive Cohort**").

2.3 Subject to the Supplier's compliance with the provisions of this Contract, the Authority shall not, during the Term, authorise any third party to provide goods and/or services equivalent to the Services in relation to the whole or any part of an Exclusive Cohort.

2.4 The Supplier acknowledges and agrees that during the Term the Authority may, subject to clause 2.3, authorise a third party to provide goods and/or services equivalent to the Services in relation to the TQ in England to students in cohorts outside the Exclusive Cohort, notwithstanding the continuation of the Services under this Contract in respect of any Exclusive Cohort.

2.5 The Supplier shall, subject to clause 15 (*Ending or extending this Contract*), be responsible for providing the Services to Students who are within an Exclusive Cohort until the later of the end of their TQ and 2 years following the end of the final Academic Year of the TQ for the Exclusive Cohort of which such Student was part.

2.6 Unless otherwise agreed with the Authority in writing, the TQ shall be offered by the Supplier on the basis that teaching of the TQ by Providers for each Exclusive Cohort will commence in September of the relevant Academic Year (accepting that Students may, subject to applicable Supplier and Provider rules, commence their study of the relevant TQ later than the teaching commencement date).

3 How the Services must be supplied

3.1 The Supplier must provide the Services:

3.1.1 in full compliance with the Service Requirements and the Supplier's Response, provided always that:

(i) the fact that the Supplier has complied with the Supplier's Response shall not limit the Supplier's obligation to satisfy the Service Requirements; and

(ii) the fact that the Supplier has satisfied the Service Requirements shall not limit the Supplier's obligation to comply with the Supplier's Response;

3.1.2 to a professional standard;

3.1.3 with reasonable skill and care;

3.1.4 using Good Industry Practice;

3.1.5 in accordance with its own policies, processes and quality control measures to the extent that these do not conflict with this Contract;

3.1.6 in accordance with any agreed timings set out in this Contract;

3.1.7 in accordance with Law;

3.1.8 in accordance with the Conditions of Recognition;

3.1.9 in a manner that ensures that neither it, nor any of the Supplier Staff:

(i) brings the Authority, the Department or the ESFA into disrepute by engaging in any act or omission which is reasonably likely to diminish the trust that the public places in any or all of them; and/or

(ii) engages in any act or omission which is reasonably likely to bring the T Levels Programme into disrepute,

in either case, regardless of whether or not such act or omission is related to the Supplier's obligations under this Contract; and

3.1.10 in accordance with (and in a manner consistent with enabling the Supplier and the T Level Awarding Organisations to achieve the aims set out in) Schedule 4 (*Co-operation*).

3.2 The Supplier must:

3.2.1 co-operate and, where appropriate, consult with the Stakeholders and the Authority's third-party suppliers, including but not limited to the Former Supplier, on all aspects connected with the delivery of the Services; and

3.2.2 ensure that Supplier Staff comply with any reasonable instructions of the Authority in relation to the Services.

Ofqual Recognition

3.3 The Supplier must have in place from the Effective Date and maintain throughout the Term, Ofqual Recognition.

3.4 The Supplier must comply with each Condition of Recognition throughout the Term.

Impact of approval by the Authority

3.5 The Supplier agrees and accepts that except for confirmation of a Variation pursuant to clause 28 (*Changing this Contract*), which expressly changes the Supplier's obligations or liabilities or the Authority's rights under this Contract, no review, comment, authorisation to proceed (as contemplated by clause 5.11.1) or approval by the Authority (including any IfATE Approval) in connection with any Product and/or Service (including in respect of the Supplier's Response, the Implementation and Delivery Plan, the Resource Plan and any documents or information submitted by the Supplier in order to obtain IfATE Approval) shall operate to exclude or limit the Supplier's obligations or liabilities or the Authority's rights under this Contract, and:

3.5.1 the Supplier retains sole responsibility for ensuring that the TQ (including the Products and Services) meets and continues to meet all relevant

Service Requirements (as they may be amended from time to time in accordance with this Contract) throughout the Term; and

3.5.2 the Supplier acknowledges and accepts that any review, comment, authorisation to proceed or approval (including any IfATE Approval) do not constitute or imply any warranty from the Authority or Ofqual in respect of the TQ.

4 Pricing and payments

4.1 In exchange for the provision of the Services (including the supply of the Products), the Supplier must invoice:

4.1.1 the Authority for the relevant Charges, which, in the case of:

(i) the Development Charge, shall be invoiced by the Supplier at the time and in the manner set out in clauses 5.11.1(ii), or 5.13.1(ii) (*Developing the TQ and achieving IfATE Approval*) (as applicable));

(ii) that part of the Charges referred to in limb (b) of the definition of Charges, shall, unless otherwise agreed by the Authority, be invoiced by the Supplier on IfATE Approval of the relevant TQ Change; and

(iii) that part of the Charges referred to in limb (c) of the definition of Charges, shall be invoiced by the Supplier as set out in the relevant Variation; and

4.1.2 the Approved Providers for the Fees pursuant to the applicable Provider Contract.

4.2 The Supplier acknowledges and agrees that:

4.2.1 in no circumstances shall the Authority, the Department or ESFA have any liability to the Supplier in respect of the Fees. The Authority is not liable if any Provider (or other third party) fails to pay any fees or other costs (including the Fees) due from them to the Supplier; and

4.2.2 save as permitted by the relevant Provider Contract, the Supplier shall not be entitled to levy any costs and/or charges and/or require any further

and/or additional payment in respect of the provision of the Services (including the supply of any Products) to any Approved Provider (and/or any Student) other than the Fees.

4.3 All Fees and Charges:

4.3.1 exclude VAT, which is payable on provision of a valid VAT invoice to the applicable payor; and

4.3.2 include all costs payable by the Authority and/or any Provider (as the case may be) in connection with the Services (including the supply of the Products).

4.4 The Authority must pay the Supplier:

4.4.1 in respect of the Development Charge, the relevant Interim Milestone Payment or the Final Milestone Payment (as the case may be); or

4.4.2 in respect of any other Charges arising under clause 8 (*TQ Changes*) or clause 28 (*Changing this Contract*), the amount of any such Charges due under such clause 8 (*TQ Changes*) or clause 28 (*Changing this Contract*),

in each case, within 30 days of receipt by the Authority of a valid, undisputed invoice, in cleared funds to the account as notified by the Supplier to the Authority.

4.5 A Supplier invoice is only valid if it includes this Contract reference and purchase order number (if any) and other details reasonably requested by the Authority.

4.6 If there is a Dispute between the Parties as to the amount invoiced by the Supplier to the Authority, the Authority must pay the undisputed amount. The Supplier cannot suspend the provision of the Services (including the supply of the Products) unless the Supplier is entitled to terminate this Contract for a failure to pay undisputed sums in accordance with clause 15.5 (*When the Supplier can end this Contract*). Any disputed amounts shall be resolved through the Dispute Resolution Procedure.

4.7 If a payment of an undisputed amount is not made by the Authority by the due date, then the Authority shall pay the Supplier interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.

4.8 The Supplier can issue a written Reminder Notice to the Authority (in accordance with clauses 29.129.1 and 29.2 (*How to communicate about this Contract*)) if the Authority does not pay an undisputed invoice on time.

4.9 The Authority may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.10 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, the Authority can publish the details of the late payment or non-payment. The Supplier must also ensure that any Sub-Contract it enters into contains provisions which have the same effect as clauses 4.4, 4.6, 4.7 and this clause 4.10.

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless a court orders this.

Indexation of Fees and Rate Card rates

4.12 The Supplier shall be entitled to adjust the Fees and the Rate Card rates which apply in respect of any Academic Year following the Academic Year in which the TQ is launched in accordance with the provisions of clause 4.13 to reflect the impact of inflation.

4.13 Where the Supplier wishes to adjust the Fees and/or Rate Card rates in accordance with clause 4.12:

4.13.1 the Supplier shall notify the Authority in writing of the proposed percentage adjustment in the existing Fees and/or Rate Card rates and the resulting new Fees and/or Rate Card rates by the end of February in the Academic Year prior to the Academic Year in respect of which the adjustment is to apply ("**Calculation Date**");

4.13.2 the proposed percentage adjustment to the relevant then current Fees or Rate Card rates must be no greater than the percentage increase in the preceding 12 months of the UK Consumer Price Index most recently published by the UK Office of National Statistics prior to the Calculation Date; and

4.13.3 the proposed adjustment calculated in accordance with this clause 4.13 shall not operate to adjust the Fees or Rate Card rates for the then current Academic Year, but shall operate to adjust the Fees or Rate Card rates as applicable with effect from the immediately following Academic Year.

4.14 In addition to any changes to the Entry Fee by virtue of clause 4.13, the Entry Fee may be subject to change from time to time, in accordance with the provisions set out in Schedule 6A.

4.15 Except as set out in clause 4.13, neither the Charges, the Fees nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier or Subcontractors of the performance of their obligations under this Contract.

5 Developing the TQ and achieving IfATE Approval

5.1 The Supplier shall develop the TQ to meet the Service Requirements and in accordance with the terms of this Contract.

Requirement for IfATE Approval

5.2 The Supplier acknowledges and accepts that:

5.2.1 the Supplier shall not make the whole or any part of the Initial TQ Deliverables available to Eligible Providers and/or Approved Providers for delivery to Students until IfATE Approval has been granted; and

5.2.2 the Supplier shall, where possible, (and in each case with the prior written consent of the Authority) share draft versions of the Initial TQ Deliverables and Guide Standard Exemplification Materials, with Eligible Providers and/or Approved Providers to support their preparations to deliver the TQ.

General development obligations

5.3 The Supplier must:

5.3.1 design and develop the TQ in accordance with paragraphs 2.1 and 2.2 of Part 1 of the Service Requirements and in order to meet the Milestones;

5.3.2 consult with:

(i) the Authority, the Department, ESFA and the Route Panels; and

(ii) a representative sample of Providers and Employers,

in the design and development of the TQ (including as contemplated by paragraph 2.1.4 of the Service Requirements);

5.3.3 take into account any input received from the Route Panel, and where applicable, the T Level Panels in the design and development of the TQ, and consult as appropriate with the T Level Panels and/or the Route Panel prior to the first Interim Milestone;

5.3.4 co-operate (as required) and work collaboratively with the Authority to achieve IfATE Approval of the TQ;

5.3.5 take into account the Technical Qualifications Service Requirements Explanatory Note together with any guidance as issued by the Authority from time to time in the design and development of the TQ, and provide input when reasonably requested by the Authority to support the development and updating of such Technical Qualifications Explanatory Note; and

5.3.6 submit to the Authority an updated Implementation and Delivery Plan and Resource Plan within 5 Working Days from the Effective Date.

Development support from the Authority

5.4 The Supplier Authorised Representative and/or senior representatives of the Supplier's development team as appropriate will meet monthly (or more frequently if deemed necessary by the Authority) with the Authority Authorised Representative and/or representatives of the Authority's Commissioning & Development Team, at a time and location to be advised by the Authority, following the Effective Date until IfATE Approval of the TQ (each a "**TQ Development Meeting**") to review progress on TQ development, address key risks and identify solutions to any barriers to progress. The Authority shall issue an agenda in advance of each TQ Development Meeting. In the event that the development of the TQ is materially delayed against the Milestones and/or the dates given in the Implementation and Delivery Plan, on a written request

by the Authority the Supplier's Chief Executive Officer or an equivalently senior individual shall attend the next TQ Development Meeting.

5.5 The Supplier shall:

5.5.1 not less than 5 Working Days prior to each TQ Development Meeting, submit the Development Phase Report to the Authority in respect of the relevant month, together with, without prejudice to paragraph 2.5 of Part 1 of the Service Requirements:

(i) updated versions (meeting all of the requirements of the relevant Product Description) of the following Products:

(A) the Implementation and Delivery Plan;

(B) the Resource Plan;

(C) the Risk Register; and

(D) the Issues Log; and

(ii) as requested by the Authority from time to time, the then current versions of the following:

(A) the TQ Specification;

(B) the Assessment Strategy;

(C) the TQ Specimen Assessment Materials;

(D) the Guide Standard Exemplification Materials;

(E) the Provider Approval Criteria;

(F) the Submission Issues Log;

(G) Employer & Provider Engagement Strategy; and

(H) any draft version of the Key Dates Schedule that the Supplier intends shall (if Approved) become the Key Dates Schedule for the purposes of this Contract from time to time,

it being understood that the Supplier will not be in breach of this clause 5.5.1 if the relevant item is still being developed and the Milestone for its completion has not been reached as at the date of the relevant TQ Development Meeting; and

5.5.2 provide a verbal summary at each such TQ Development Meeting of the progress of development of the TQ as against the Implementation and Delivery Plan and Resource Plan and any identified risks to the on time delivery of the TQ and proposed resolutions.

5.6 The Authority shall provide minutes setting out an accurate summary of each such TQ Development Meeting within 5 Working Days of each such meeting.

Submission process

5.7 The Supplier shall, on or prior to the applicable Submission Date, make all Submissions to the Authority necessary in respect of IfATE Approval in accordance with paragraphs 2.1 and 2.2 of Part 1 and Annex 7 to the Service Requirements.

5.8 The Supplier shall ensure that all Submissions made in accordance with clause 5.7 meet all of the requirements for each Submission as set out in paragraph 2.1 of Part 1 and Annex 7 to the Service Requirements. Unless notified otherwise by the Authority in writing, the Supplier shall continue its ongoing work in relation to the Initial TQ Deliverables following each Submission whilst such Submission is being considered by the Authority and/or Ofqual. For the avoidance of doubt, this means that the Supplier, following each Submission for each Interim Milestone, shall not await notification from the Authority in accordance with Clause 5.11 below before continuing work on the Initial TQ Deliverables required for any subsequent Milestone.

5.9 The Supplier shall submit to the Authority for Approval, a final version of the Guide Standard Exemplification Materials in accordance with paragraph 2.1 of Part 1 and Annex 7 to the Service Requirements.

5.10 The Supplier shall respond promptly to the Authority to any requests from the Authority for further information to support any Submission and/or the IfATE Approval process.

5.11 In respect of each Interim Milestone, the Authority and, if relevant, Ofqual will consider each Submission made in accordance with clause 5.7 and 5.8 and, within a timeframe

which should allow the TQ to be developed in time for delivery in accordance with this Contract:

5.11.1 if the Authority considers that the Submission (or Re-Submission (as the case may be)) meets all of the requirements of paragraphs 2.1 and 2.2 of Part 1 and Annex 7 to the Service Requirements for the relevant Interim Milestone, the Authority shall:

(i) confirm in writing to the Supplier that such requirements have been met; and

(ii) where the relevant Interim Milestone attracts an Interim Milestone Payment, pay to the Supplier (in accordance with clause 4 (*Pricing and payments*)) the applicable Interim Milestone Payment; or

5.11.2 if (1) the Authority does not consider that the Submission (or Re-Submission (as the case may be)) meets all of the requirements of paragraphs 2.1 and 2.2 of Part 1 and Annex 7 to the Service Requirements for the relevant Interim Milestone and/or (2) the Supplier has outstanding issues still to be addressed / additional information still to be provided in relation to any previous Interim Milestones (including in relation to any previous Interim Milestones that do not attract an Interim Milestone Payment), the Authority may withhold payment to the Supplier of the applicable Interim Milestone Payment (if any) and shall:

(i) notify the Supplier of the issues that need to be addressed and/or the additional information that needs to be provided (and, acting reasonably, the date by which such issues need to be addressed and/or such information needs to be provided) and whether the Authority will be withholding payment of the applicable Interim Milestone Payment (if any), and the Supplier shall promptly address such issues and resubmit the relevant documentation and/or provide such additional information (a "**Re-Submission**") to the Authority on or prior to the date notified by the Authority, following which clause 5.11.1 or this clause 5.11.2 will apply to such Re-Submission; or

(ii) notify the Supplier:

(A) that notwithstanding the failure of the Submission (or Re-Submission (as the case may be)) to meet all of the requirements of paragraphs 2.1 and 2.2 of Part 1 and Annex 7 to the Service Requirements for the relevant Interim Milestone, the Supplier shall continue with the design and development of the TQ without having to make a Re-Submission, provided that the relevant issues are addressed by any timescales specified by the Authority and in any event no later than by the Final Approval Milestone Date; and

(B) whether the Authority will be withholding payment of the applicable Interim Milestone Payment (if any), following which the Supplier shall promptly address the issues identified / further information required, as part of its ongoing development of the TQ in accordance with the timescales specified by the Authority. If the Authority is withholding payment of any applicable Interim Milestone Payment, subject to the Supplier having addressed the issues identified in accordance with the required timescales (and in any event no later than by the Final Approval Milestone Date), clause 5.11.1(ii) will apply.

5.12 The Supplier acknowledges and agrees that owing to the meeting dates scheduled for the IfATE Approval process, any delay in making the Final Submission to the Authority by the Final Approval Milestone Date may cause a delay of several weeks for IfATE Approval. Accordingly, failure by the Supplier to make the Final Submission in accordance with clause 5.7 and/or 5.8 by the Final Approval Milestone Date, other than due to a breach of this Contract by the Authority, shall be a Critical Service Failure.

5.13 In respect of the Final Approval Milestone, the Authority and, if relevant, Ofqual will consider the Final Submission made by the Supplier in accordance with clause 5.7 and 5.8 and, within a timeframe which should allow the TQ to be developed in time for delivery in accordance with this Contract:

5.13.1 if the Authority considers that the Final Submission (or Final Re-Submission (as the case may be)) meets the requirements for IfATE Approval, then the Authority shall:

(i) confirm to the Supplier in writing that the TQ has IfATE Approval and that, subject (if applicable) to clause 7.2 (*Interaction with* Providers) and clause 14.3.1 (*What may happen if there are issues with your provision of the Services*), the Supplier is authorised to proceed to make the TQ available to Approved Providers for delivery to Students in accordance with clause 6 (*Operating the TQ*); and

(ii) pay to the Supplier (in accordance with clause 4 (*Pricing and payments*)) the Final Milestone Payment, together with any outstanding Interim Milestone Payments or;

5.13.2 if the Authority considers that the Final Submission (or Final Re-Submission (as the case may be)) does not meet the requirements for IfATE Approval, then the Authority shall either

(i) notify the Supplier in writing of the issues that need to be addressed and/or the additional information that needs to be provided and the Supplier shall within 10 Working Days (or such longer timeframe as is agreed in writing by the Authority) address such issues and resubmit the relevant documentation and/or provide such additional information, following which this clause 5.13 will apply to such Final Re-Submission or

(ii) take any other steps available to it under the contract.

5.14 The Supplier acknowledges and accepts that the Authority will share, as it deems necessary, with Ofqual, the Department, ESFA, and the Route Panel:

5.14.1 all Submissions (including any Final Submission) and/or Re-Submissions (including any Final Re-Submissions) submitted by the Supplier under clause 5.7 and/or clause 5.13;

5.14.2 any information required by the Authority pursuant to clause 5.10;

5.14.3 any information required by Ofqual for the Regulation of the TQ or to perform the statutory functions of Ofqual; and/or

5.14.4 any other information it holds in relation to the Supplier,

and the provisions of clause 19 (*What must be kept confidential*) will not prevent any disclosure or sharing of documentation and/or information by the Authority under this clause 5.14.

6 Operating the TQ

6.1 Following IfATE Approval the Supplier must (subject to clause 7.2 (*Interaction with Providers*) and clause 14.3.1 (*What may happen if there are issues with your provision of the Services*)) make the TQ (including (as applicable) the Products) available to Approved Providers for delivery to Students and provide the Services (other than the Initial Development Services) in accordance with the Service Requirements.

6.2 The Supplier shall meet all KPIs in the delivery of the Services (other than the Initial Development Services).

6.3 The Supplier must comply with the current version of any Key Dates Schedule in respect of the making available of the TQ and the performance of the Services (other than the Initial Development Services).

6.4 The Supplier must provide materials and Student Information to the Authority in accordance with paragraphs 5, 8 and 10 of Part 1 of the Service Requirements to enable the Authority to keep a record in the event such materials and/or information is required for the transfer of Services to a Replacement Supplier.

6.5 The Supplier shall promptly provide to the Authority such materials relating to the TQ and Student Information as are requested in writing by the Authority to enable work by or on behalf of the Authority and/or Ofqual to ensure the ongoing maintenance between Cohorts of the grades and standards of the TQ and the wider T Level Programme.

6.6 The Supplier shall actively promote the TQ to Eligible Providers.

7 Interaction with Providers

7.1 The Supplier shall, in accordance with the requirements set out in paragraph 3 of Part 1 of the Service Requirements, operate a procedure to receive applications for Provider

Approval from Eligible Providers that wish to make the TQ available to Students, and where the relevant Provider Approval Criteria are met to grant Provider Approval and notify the Approved Providers accordingly. The Supplier acknowledges and agrees that:

7.1.1 it shall not be entitled or permitted to:

(i) charge any additional costs, charges and/or fees arising out of or in connection with the implementation and operation of such procedure and/or the granting of Provider Approval; and/or

(ii) impose any additional requirements (other than a Provider Contract) on any Eligible Provider and/or Approved Provider (as applicable) as a condition to and/or consequence of the grant of Provider Approval;

7.1.2 only an Eligible Provider shall be eligible to be granted Provider Approval by the Supplier in respect of the TQ; and

7.1.3 subject to clause 7.1.2 and without prejudice to paragraph 3.1.1 of Part 1 of the Service Requirements, the Supplier shall promptly grant Provider Approval to Eligible Providers who meet the Provider Approval Criteria following receipt of their application for Provider Approval.

7.2 The Supplier shall review and assess Approved Providers on an ongoing basis in accordance with paragraph 3.1.2 of Part 1 of the Service Requirements to ensure that they continue to meet the requirements for Provider Approval to make the TQ available to Students and, subject to the provisions of paragraphs 3.2 to 3.5 (inclusive) of Part 1 of the Service Requirements, where an Approved Provider no longer meets the Provider Approval Criteria, the Supplier shall revoke such Provider Approval.

7.3 The Supplier shall ensure that:

7.3.1 prior to any Eligible Provider making the TQ available to Students:

(i) the Eligible Provider is an Approved Provider;

(ii) a binding Provider Contract is in place with the relevant Approved Provider; and

7.3.2 the Provider Services shall only be provided to an Approved Provider during the term of, and subject to the provisions of, the applicable Provider Contract.

7.4 Without prejudice to paragraph 5 of Part 1 of the Service Requirements, the Supplier shall promptly register a Student for the TQ following receipt by the Supplier of an application for registration of that Student from an Approved Provider.

7.5 The Supplier shall, on written request by the Authority, promptly provide a copy of each Provider Contract to the Authority and to the Department and/or the ESFA.

7.6 The Supplier shall retain copies of all documentation and information in relation to arrangements with Eligible Providers and Approved Providers, including all such documentation and/or information arising out of or in connection with:

7.6.1 the application for and/or the grant of Provider Approval referred to in clause 7.1; and

7.6.2 the ongoing monitoring of Approved Providers by the Supplier referred to in clause 7.2,

and without prejudice to the generality of the definition of IfATE Data, such documentation and information shall form part of the IfATE Data to which the provisions of clause 18 (*Data protection and information*) shall apply.

7.7 The Supplier shall make available the Additional Services and provide the Additional Services on request by Approved Providers in accordance with paragraphs 5, 6, and 9 of Part 1 of the Service Requirements.

7.8 The Supplier shall be permitted to offer and provide additional products and/or services in each case related to the TQ to Approved Providers (and Students), provided always that:

7.8.1 such additional products and services are not identical to, or performing an equivalent function in relation to the TQ to, the whole or any part of the Products and/or the Services (including the Additional Services) and offered and/or provided on alternative terms and/or conditions (including as to timing or quality) to those terms and conditions which would apply pursuant to this Contract to the applicable Products and/or Services;

7.8.2 without prejudice to clause 7.1.1(ii) and the requirements of Schedule 17 (*Provider Contract Requirements*), the Supplier shall not, other than the Provider Contract, impose any condition on any Eligible Provider (including any Approved Provider) and/or Student to purchase such additional products and/or services as a condition to and/or consequence of:

(i) the grant of any Provider Approval; and/or

(ii) the proper performance of any of the Services (and/or the supply of any Products); and

7.8.3 the Supplier shall not (in making available such products and/or services available and/or in respect of the terms on which such products and/or services are made available) favour one Provider and/or group of Providers or one Student and/or group of Students over another.

7.9 The Supplier shall comply with Schedule 17 (*Provider Contract Requirements*) in respect of its contracts with Approved Providers in relation to the TQ.

8 TQ Changes

8.1 The Supplier acknowledges and agrees that the Authority may request changes to the TQ and that the Authority may publish revised Outline Content from time to time.

8.2 The Supplier must ensure that the Approved Initial TQ Deliverables reflect the version of the Former Supplier's TQ Specification as at the Effective Date ("**Initial Content Date**") and that the Approved Initial TQ Deliverables reflect any TQ Change requested by the Authority before IfATE Approval.

8.3 The Supplier must make any TQ Change reasonably requested by the Authority to reflect any changes to the Former Supplier's TQ Specification or ,if relevant, the Outline Content following the Initial Content Date subject to the terms of this clause 8.

8.4 The Authority may carry out annual reviews in each Academic Year where a new Cohort is commencing the TQ in the following Academic Year to identify any potential TQ Changes required by the Authority. The Authority may prepare and submit to the Supplier by the relevant dates prescribed by the TQ Content Updating Schedule in each such Academic Year up to two annual guidance notes setting out the output of the Authority's reviews in relation to Inclusive TQ Changes and Exclusive TQ Changes

respectively. Where the Authority identifies any potential TQ Change (in an annual guidance note or otherwise), the Authority shall promptly notify the Supplier in writing of details of the potential TQ Change.

8.5 Without prejudice to paragraphs 2.5 and 2.6 of Part 1 of the Service Requirements which shall apply in addition to any annual review, the Supplier shall carry out an annual review of the TQ once in each Academic Year, taking into account the output of any Authority annual guidance note(s) pursuant to clause 8.4 and any additional updates the Supplier has proposed to the TQ (to the extent that such updates have not otherwise been Approved pursuant to paragraph 2.5 or 2.6 of Part 1 of the Service Requirements), to identify any potential TQ Changes required to ensure ongoing compliance of the TQ with the Service Requirements. Where the Supplier identifies any potential TQ Change, the Supplier shall promptly notify the Authority in writing of details of the potential TQ Change.

8.6 Where a TQ Change is an Exclusive TQ Change, the Parties shall follow the Variation procedure set out in clause 28 (*Changing this Contract*) in respect of the relevant Exclusive TQ Change. The Charges relating to such Exclusive TQ Change shall be agreed between the Parties as part of the Impact Assessment for the relevant Variation, each Party acting reasonably and promptly, prior to the Supplier commencing work on the Exclusive TQ Change. The relevant Charges shall:

8.6.1 be a reasonable cost for implementing the Exclusive TQ Change in the circumstances;

8.6.2 take into account and be calculated using:

(i) for personnel related costs and other relevant charges which are set out in the Rate Card, the applicable Rate Card rates; and

(ii) reasonable charges for any non-personnel related costs which are not included in the Rate Card and which will be incurred by the Supplier to implement the Exclusive TQ Change; and

8.6.3 be consistent with the costs applicable to any relevant costed change scenario set out in Schedule 6 (*Pricing Schedule*) or, where no costed change scenario for the applicable TQ Change is set out in Schedule 6 (*Pricing Schedule*), be calculated on the same basis and using the same

logic and inputs as those which applied to determine the costs for the costed change scenarios, as such logic and inputs may be amended only to the extent as is necessary to reflect the TQ Change in question.

8.7 Where the TQ Change is an Inclusive TQ Change, the Supplier shall implement such Inclusive TQ Change at the cost of the Supplier and there shall be no additional Charges or Fees as a result of such Inclusive TQ Change.

8.8 The Supplier shall obtain the Authority's prior written agreement before implementing any TQ Change which, in the case of an Exclusive TQ Change, shall be in the form of an executed Variation to this Contract. Following such agreement the Supplier shall, unless otherwise agreed with the Authority, implement:

8.8.1 Inclusive TQ Changes such that the updated TQ is ready for teaching to new Students in the next Academic Year following the date of such agreement; and

8.8.2 Exclusive TQ Changes such that the updated TQ is ready for teaching to new Students in the second Academic Year following the date of such agreement,

provided that in each case that the Supplier shall continue to make available the version of the TQ prior to such TQ Change as is necessary to support continuing Students who commenced their studies on such version of the TQ prior to the implementation of such TQ Change.

8.9 The Supplier shall consult with a representative sample of relevant Employers and take into account the output of consultation with such Employers as appropriate in relation to any TQ Change in accordance with the Service Requirements and shall provide the Authority with evidence of such consultation.

8.10 If the Supplier makes any Inclusive TQ Changes, the Supplier must resubmit the TQ documentation including any Products (as amended to reflect the TQ Change in question) to the Authority for agreement by the relevant date prescribed by the TQ Content Updating Schedule, unless otherwise agreed with the Authority, before (where applicable) making the relevant revised version of the TQ available to Approved Providers for delivery to Students.

8.11 If the Supplier makes any Exclusive TQ Changes, the Supplier must resubmit the TQ documentation including any Products (as amended to reflect the TQ Change in question) to the Authority for IfATE Approval by the relevant date prescribed by the TQ Content Updating Schedule, unless otherwise agreed with the Authority, before (where applicable) making the relevant revised version of the TQ available to Approved Providers for delivery to Students and the provisions of clause 5.13 shall apply to such amended TQ documentation as if references to the "Final Submission" (or "Final Re-Submission" (as the case may be)) in that clause 5.13 are references to the "TQ documentation including any Products (as amended to reflect the TQ Change in question)"; reference to the "Final Approval Milestone" is a reference to the "TQ Change in question"; and references to payment refer to payment of any charges agreed in the applicable Variation.

8.12 Unless otherwise agreed with the Authority in writing, any agreed or approved (as the case may be) updates to the TQ must (where applicable) be made available to Approved Providers by the Supplier by the relevant date prescribed by the TQ Content Updating Schedule.

9 Record keeping, monitoring and reporting

9.1 Without prejudice to clause 5.5 (*Developing the TQ and achieving IfATE Approval*) and clause 7.6 (*Interaction with Providers*), the Supplier shall:

9.1.1 monitor and report (in an Operational Delivery Report) its performance of the Services (other than the Initial Development Services) in accordance with Schedule 15 (*Monitoring of Performance*) and the Parties agree that the provisions of such Schedule 15 (*Monitoring of Performance*) shall apply to determine (amongst other things) the process following (and the outcome of) such monitoring and reporting (including in relation to the carrying out of the Performance Review Meeting and the requirement for and consequences of any KPI Improvement Plan); and

9.1.2 comply with the record keeping and reporting obligations set out in paragraphs 5, 8 and 10 of Part 1 of the Service Requirements.

9.2 The Supplier must allow, and must ensure that any Key Subcontractor allows, any Auditor access to the Supplier's or Key Subcontractor's premises and/or systems

(including IT systems), as relevant, to Audit everything to do with this Contract and/or to obtain any information required in relation to any investigation by Ofqual.

9.3 The Supplier must provide, and must ensure that any Key Subcontractor provides, information to the Auditor and reasonable co-operation at the Auditor's request to enable any Audit to be undertaken.

9.4 The Supplier must create and maintain throughout the Term a full and accurate version control log recording all TQ Changes made during the Term.

9.5 The Supplier shall maintain and shall promptly, following a written request by the Authority, provide to the Authority, the following:

9.5.1 the Supplier's detailed and up to date cost model for the provision of the Services under this Contract including a future projection for the remaining Term;

9.5.2 details of the income received by the Supplier through the provision of the Services during the Term to date, including a breakdown by service and customer and a future projection for the remaining Term; and

9.5.3 the Supplier's calculation of the overall level of profit it has achieved during the Term to date through the Services provided under this Contract.

10 Staff Transfer

10.1 The Parties agree that:

10.1.1 where the commencement of the provision of the Services or any part of the Services results in one or more Relevant Transfers, Schedule 21 (Staff Transfer) shall apply; and

10.1.2 Schedule 12 (Exit Management) shall apply on the expiry or termination of the Services or any part of the Services.

11 Supplier Staff and Subcontracting

Supplier Staff

11.1 The Supplier Staff involved in the performance of this Contract must:

11.1.1 be appropriately trained and qualified; and

11.1.2 be vetted using Good Industry Practice and, in the case of Supplier Staff referred to in paragraph 2.2 of Schedule 7 (*Staff (including Key Personnel*)), in accordance with paragraph 2 of Schedule 7 (*Staff (including Key Personnel*)).

11.2 If any default, acts, omissions, negligence and/or statements of any of the Supplier Staff involved in the performance of this Contract result in a Default, the Supplier is liable to the Authority for that Default.

11.3 Where the Authority decides (on reasonable grounds) that one of the Supplier's Staff is not suitable to work on this Contract, the Supplier must, subject to clause 11.1, promptly replace them with a suitably qualified alternative.

11.4 If requested by the Authority, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach clause 31 (*Preventing fraud, bribery and corruption*).

Subcontracting

11.5 The Supplier shall comply with the provisions of Schedule 8 (*Supply Chain (including approved Subcontractors)*) in respect of the appointment (including any proposed appointment) and/or management of any Subcontractor (including any Key Subcontractor).

11.6 Sub-contracting any part of this Contract shall not relieve the Supplier of any obligation or duty attributable to the Supplier under this Contract.

12 Rights and protection

12.1 The Supplier warrants and represents that:

12.1.1 it has full capacity and authority to enter into and to perform this Contract;

12.1.2 this Contract is executed by its authorised representative;

12.1.3 it is a legally valid and existing organisation incorporated in the place it was formed;

12.1.4 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform this Contract;

12.1.5 it maintains all necessary rights, authorisations, licences and consents to perform its obligations under this Contract;

12.1.6 it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform this Contract;

12.1.7 it is not subject to an Insolvency Event; and

12.1.8 all statements made, and documents submitted, as part of the procurement of the Services (including in the Supplier's Response) are true and accurate.

12.2 The warranties and representations in clause 12.1 are repeated each time the Supplier provides the Services and/or supplies any Products under this Contract.

12.3 The Supplier indemnifies the Authority in full against all Losses suffered or incurred by the Authority arising out of or in connection with third party claims that result from the provision of the Services including the supply of the Products.

12.4 All claims indemnified under this Contract (including for the avoidance of doubt any indemnified IPR Claim) must use the process set out in clause 30 (*Dealing with claims*).

12.5 The Authority can, even if it has made a claim in respect of the breach, still terminate this Contract for breach of any warranty or indemnity where it is entitled to do so.

12.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify the Authority.

13 Intellectual Property Rights

Vesting, ownership and licences of rights in TQ materials

13.1 The Supplier agrees to deliver such materials, and to assign or licence all IPR in such materials, as it creates, identifies for use, or uses as part of or for the Operation of the TQ to which the Authority and/or a Replacement Supplier with Relevant Competence would reasonably require access:

13.1.1 for the Authority to carry out its activities in relation to the T Level and TQ, including the approval, oversight and maintaining the integrity of the T Level and TQ;

13.1.2 for the transfer of the Operation of the TQ to a Replacement Supplier; and

13.1.3 for the Replacement Supplier to Operate (including maintaining the integrity of, modifying and developing) the TQ,

in a seamless, Transparent manner; and

13.1.4 to compete openly and effectively any future competition or tender for the Operation of the TQ or a Replacement TQ.

13.2 Without limiting the generality of clause 13.1:

13.2.1 the Supplier agrees to assign to the Authority all IPR in the Key Materials (including in Products) in accordance with the TQ Assignment and Licence;

13.2.2 the Supplier agrees to licence the Authority, with the right to sublicense, all IPR in the Ancillary Materials, in accordance with the TQ Assignment and Licence; and

13.2.3 in respect of any IPR in Key Materials, to the extent that the same are not at the relevant time vested absolutely in the Authority, the Supplier agrees to license the Authority, with the right to sublicense, such IPR in Key Materials, in accordance with the TQ Assignment and Licence.

13.3 Except as set out above or otherwise expressly provided in this Contract:

13.3.1 the Authority shall not by virtue of this Contract acquire title to or rights in any Background IPR owned by the Supplier or any third party; and

13.3.2 the Supplier shall not by virtue of this Contract acquire title to or rights in any Background IPR owned by the Authority or licensed by any third party to the Authority.

13.4 Without prejudice to the other provisions of this Contract, the assignments and licences referred to in clause 13.2 shall be subject to the terms of the TQ Assignment and Licence (during and after the Term), including the warranties and representations set

out in the TQ Assignment and Licence. The Authority and the Supplier will enter into the TQ Assignment and Licence in the form set out in Schedule 14 (*Form of Assignment and Licence*) on the Effective Date.

Rights granted to the Supplier

13.5 The Authority hereby grants to the Supplier a non-exclusive worldwide, royalty free licence with the right to sublicense, subject to, and in accordance with, the terms of this Contract, to use:

13.5.1 the Former Supplier's TQ Specification and, if relevant, the Outline Content;

13.5.2 the IfATE Data; and

13.5.3 any Authority Background IPR in other materials specifically identified for use in the provision of the Services in accordance with this sub-clause,

during the Term, solely in relation to the provision of the Services.

13.6 The Authority hereby grants to the Supplier, in so far as any relevant Intellectual Property Rights have been assigned to the Authority or are otherwise at the time vested in the Authority in accordance with clause 13.2 a worldwide, royalty free licence, with the right to sublicense, to use and exploit the IPR in the Key Materials during the Term in relation to the TQ subject to, and in accordance with, the relevant terms of this Contract.

13.7 Subject to clause 13.8, the licence to the Supplier under clause 13.6 shall be exclusive during the Term solely in respect of use of the Key Materials for the provision of the Services in respect of the Exclusive Cohorts.

Rights retained by the Authority for its activities related to the provision of the Services

13.8 The Authority will retain:

13.8.1 (for the avoidance of doubt) the non-exclusive right to use the Key Materials in its administration, approval and oversight of the TQ and other T Level technical education qualifications and to make the same available to others (such as Ofqual) to do the same; and

13.8.2 the right to use the Key Materials, and for any Future Supplier or potential Future Supplier to use the Key Materials:

(i) for competing or tendering for the delivery and Operation of the TQ and/or any Replacement TQ, where such competition or tender is for such delivery and Operation during any Transition Period and/or following expiry or termination of this Contract (ie the End Date); and

(ii) to deliver and Operate the TQ and/or any Replacement TQ, during any Transition Period; and

13.8.3 the right to sub-license others to exercise the rights set out in this clause 13.8.

Confirmation of rights, marking and branding of Materials

13.9 The Supplier shall, on any copy of any materials in which copyright belongs to the Authority, prominently mark such material with a notice saying: "Copyright in this [DOCUMENT/section of DOCUMENT] belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education [DATE]" or such other notice as the Authority may reasonably require by notice to the Supplier from time to time. Without prejudice to any rights granted to the Authority under this Contract, in the case of each Deliverable the Supplier shall deliver a certificate in the form annexed to the TQ Assignment and Licence confirming that ownership in the IPR in that Deliverable is vested in the Authority, or where it asserts that IPR in the Deliverable or certain parts of it do not vest in the Authority, identifying specifically those parts and the scope of rights it asserts the Supplier has in respect of the same.

13.10 The Supplier may use its name, logos, trade marks and/or other signs which refer to the Supplier on Key Materials and Ancillary Materials and other materials used in the Operation of the TQ or to promote the TQ which are of the type set out in the T Level Branding Guidelines, provided that any such use shall be strictly as set out in the T Level Branding Guidelines. Without prejudice to the last sentence, the Supplier shall, on notice from the Authority, provide representative samples of all such use, and, if the notice so requests, provide such samples a reasonable period in advance of any proposed such use together with a period (not being less than 7 Working Days) for comment. The Authority may notify the Supplier within such period of any comments,

including any requirements it has in respect of such use, and, the Supplier shall take reasonable account of any such comments and comply with any reasonable requirements of the Authority so notified.

13.11 The Supplier shall not use its name, logos, trade marks and/or other signs which refer to the Supplier, in a trade mark manner or as any designation of origin, on any material referred to in clause 13.10 or otherwise in connection with its Operation of T Levels or T Level technical education qualifications (including the TQ), except as provided in clause 13.10 or otherwise with the specific Approval of the Authority; and in any event any use of its name, logos, trade marks and/or other signs which refer to the Supplier in connection with the T Level or T Level technical education qualifications (including the TQ) shall not be such as to make, suggest or imply any connection between the Authority or any T Levels or any T Level technical education qualifications and the Supplier, or endorsement by the Authority or the Department, other than as arises under this Contract or any other contract for the supply of T Level technical education qualifications.

13.12 The Supplier shall:

13.12.1 apply to all Key Materials and Ancillary Materials provided to any third party, the Authority's name and logo in such manner as is reasonably prescribed from time to time in writing by the Authority; and

13.12.2 use in respect of the TQ, including, unless otherwise agreed with the Authority, on all Key Materials and Ancillary Materials, such descriptive name (for example in the form: "[technical qualification] in Construction") as is determined by the Authority or proposed by the Supplier and agreed by the Authority,

provided that such use shall at all times be in strict accordance with the other provisions of this Contract, the T Level Trade Mark Licence, and any style guides or other instructions issued from time to time by the Authority.

Supplier's operation of other qualifications

13.13 The Supplier shall not, within or outside England, offer or promote any qualification other than the TQ as:

13.13.1 being the TQ (or any other technical qualification forming part of a T Level) or T Level (or part of a T Level);

13.13.2 being identical in terms of content and assessment requirements to the TQ (or any other technical qualification forming part of a T Level) or T Level and/or including identical components to the TQ (or any other technical qualification forming part of a T Level) or T Level; or

13.13.3 demonstrating the same level of occupational competence as the TQ (or any other technical qualification forming part of a T Level) or T Level,

provided always that nothing in this Contract shall prevent the Supplier from offering or promoting the technical qualification element of a T Level under a separate contract with the Authority in connection with the making available of that technical qualification.

13.14 The Supplier may only re-use the whole of the TQ in an un-amended or materially un-amended form, other than as part of the Services during the Term, as follows:

13.14.1 in the Operation of qualifications for any of the Devolved Administrations, with the specific Approval of the Authority;

13.14.2 in the Operation of qualifications in England intended for and only marketed to students who are not in the category known as “16 to 19 year old”, with the specific Approval of the Authority; and

13.14.3 in the Operation of qualifications outside the UK, save in any jurisdictions the Authority excludes by notice to the Supplier,

provided in each case that the name “T Level” is not used in the qualification or any marketing or promotion of the qualification, and that it is at all times clear and made clear to students and other third parties that the qualification does not form and cannot be used as any part of a T Level.

13.15 Subject to clauses 13.13 and 13.14, nothing in this Contract or the TQ Assignment and Licence shall restrict or prevent the Supplier from continuing to offer and update its existing qualifications (including technical qualifications), from offering new technical qualifications, or from using elements of the Key Materials in the operation of qualifications other than the TQ.

Dealing with intellectual property claims

13.16 If there is an IPR Claim, the Supplier indemnifies the Authority against all Losses suffered or incurred by the Authority as a result.

13.17 Where a Party acquires ownership of IPR incorrectly under this Contract it must do everything reasonably necessary to complete a transfer in writing assigning the IPR to the other Party on request and at its own cost.

13.18 Clause 13.16 shall not apply to the extent that the IPR Claim is caused by the Authority's use of the relevant IPR in breach of the terms of this Contract.

13.19 In the event that any Third Party IPR is included in the Key Materials, Ancillary Materials, or other Deliverables under this Contract, the Supplier shall ensure that it has or acquires sufficient rights to any such Third Party IPR to enable it to enter into any applicable assignments and to grant any applicable licences under this Contract.

Portability of the TQ

13.20 The Supplier shall, where possible, ensure that its design and development of the TQ enables the transfer of the materials described in clause 13.1 to a Future Supplier without requiring use by such Future Supplier of any underlying proprietary system or platform which does not form part of the Key Materials or Ancillary Materials.

14 What may happen if there are issues with your provision of the Services

14.1 The Supplier must notify the Authority promptly in writing if:

14.1.1 it becomes aware of any problem or complaint from any individual or organisation in relation to the making available and/or operation of the TQ;

14.1.2 it makes any changes to its management, governance, organisational and/or operational structure or capacity from that which is set out in the Supplier's Tender which shall or may be material to the provision of the Services;

14.1.3 it undergoes or proposes to undergo (or, without prejudice to clause 15.7 (*When Sub-Contracts can be ended*) becomes aware that a Subcontractor has undergone or proposes to undergo) a change of Control;

14.1.4 there is a material adverse change in the financial circumstances of the Supplier, the Supplier becomes aware of a material adverse change in the financial circumstances, or the Supplier has (or anticipates that it may have) insufficient funding to adequately resource its obligations under this Contract;

14.1.5 it becomes aware of any circumstances relating to the Supplier or any Subcontractor which shall or may bring into disrepute and/or diminish the trust that the public places in the Authority, the Department or the ESFA and/or the T Levels Programme (including any Conflict of Interest (as contemplated by clause 36 (*Conflict of interest*)) and/or any child protection and/or data handling issues and/or incidents);

14.1.6 it becomes aware of any issue which shall or may have an adverse impact on Students studying for the TQ;

14.1.7 it is required, pursuant to the Conditions of Recognition, to notify Ofqual of any event that has occurred (or is likely to occur) which it has cause to believe could have an "Adverse Effect" (as defined in the Conditions of Recognition);

14.1.8 any of the circumstances in clause 15.7 (*Ending or extending this Contract*) occur; or

14.1.9 a Critical Service Failure occurs.

14.2 If:

14.2.1 the Supplier has failed to make the Submission for the relevant Interim Milestone on or prior to the Submission Date for that relevant Interim Milestone;

14.2.2 the Authority reasonably believes that:

(i) the Supplier is not likely to achieve IfATE Approval by the Final Approval Milestone Date;

(ii) the Authority is likely to need to withdraw IfATE Approval;

(iii) Ofqual is likely to need to withdraw Ofqual Recognition;

14.2.3 the Authority has obtained information giving rise to reasonable concerns about the ability of the Supplier to deliver the Services and the Authority has provided such information to the Supplier and given the Supplier a reasonable opportunity (in the circumstances) to respond to such information and any such response fails to address such concerns to the satisfaction of the Authority;

14.2.4 the Supplier fails, in the opinion of Ofqual, to comply with any Condition of Recognition;

14.2.5 the Supplier is under investigation and/or subject to regulatory enforcement by Ofqual or has had any direction issued by Ofqual in respect of it;

14.2.6 the Supplier fails to comply with and/or implement (as the case may be) the whole or any part of the Implementation and Delivery Plan in any material respect;

14.2.7 the Supplier fails to deliver the Services in accordance with the Resource Plan in any material respect;

14.2.8 the circumstances referred to in paragraph 2.3.2 of Schedule 15 (*Monitoring of Performance*) occur;

14.2.9 a Supplier Termination Event has occurred; and/or

14.2.10 any act or omission of the Supplier in relation to the TQ in breach of this Contract occurs which shall or may have a material adverse impact on Students and/or the TQ including any such act or omission which:

(i) gives rise to prejudice to Students or potential Students; or

(ii) adversely affects:

(A) the ability of the Supplier to undertake the development, delivery or award of the TQ in accordance with its Conditions of Recognition;

(B) the standards of the TQ which the Supplier makes available or proposes to make available; or

(C) public confidence in the TQ,

the Authority may issue written notification of Designated Action to the Supplier, following which the Supplier shall comply with the Designated Action in accordance with any timeframe stated in such notification. In the event that, for any reason, the Supplier is unable to comply with the Designated Action notification, the Supplier shall promptly notify the Authority and shall explain the reason why it is unable to so comply.

14.3 In the event of a Critical Service Failure, in addition to the rights of the Authority under clause 14.2 (*What may happen if there are issues with your provision of the Services*) and 15.3 (*Ending or extending this Contract*), the Authority may by serving written notice on the Supplier:

14.3.1 suspend and/or restrict any elements (in full or part) of the Services for the remainder of the Term, including a permanent prohibition or restriction on the Supplier from providing the Services (including making the TQ and/or any Products available to Approved Providers):

(i) to Cohorts (including any Exclusive Cohort) in respect of which Students are already registered for the TQ; and/or

(ii) in respect of any further Cohorts (including any Exclusive Cohort);

14.3.2 reduce the Term by one or more periods of 12 months as specified in such notice and accordingly remove one or more Cohorts from the Exclusive Cohorts; and/or

14.3.3 require the Supplier to comply with specified performance improvement conditions in relation to the Services, failing which the Term will reduce by one or more periods of 12 months as specified in such notice and the final Cohort will then be removed from the Exclusive Cohorts.

14.4 Nothing in this Contract (and no action by the Authority) shall be construed so as to limit or restrict the ability of Ofqual to take action under its statutory powers and in the event of any Dispute arising out of or in connection with Ofqual Recognition and/or any Condition of Recognition the provisions of clause 38.7 (*Resolving disputes*) will apply.

14.5 The Supplier shall provide (and shall procure that its Subcontractors provide) all information and cooperation as is required by the Authority to enable the Authority to investigate any alleged breach by the Supplier of its obligations under this Contract.

14.6 The Authority may withdraw IfATE Approval by notice in writing to the Supplier in circumstances where the requirements for IfATE Approval are no longer met by the Supplier. The Authority shall notify the Supplier in advance in writing of its proposal to withdraw IfATE Approval and shall provide a reasonable opportunity for the Supplier to make representations in relation to such proposal, and the Authority shall take such representations into account in determining whether to proceed to withdraw IfATE Approval.

15 Ending or extending this Contract

15.1 This Contract ends on the End Date.

Extending this Contract

15.2 The Authority can extend this Contract for an Extension Period by giving the Supplier written notice prior to the start of the Academic Year in which the final Exclusive Cohort commences the TQ.

When the Authority can end this Contract

15.3 If a Supplier Termination Event occurs, the Authority has the right to immediately terminate this Contract by issuing a Termination Notice to the Supplier, unless the Supplier Termination Event occurs as a result of a breach of this Contract by the Authority, but only insofar as the Authority's breach is not itself caused by a breach by the Supplier of the Supplier's obligations under this Contract.

15.4 Nothing in Clause 38 (Resolving Disputes) shall prevent or restrict the Authority from exercising its rights under clause 15.3.

What happens if this Contract ends

15.5 Where the Authority terminates this Contract, all of the following apply:

15.5.1 the Supplier shall apply to Ofqual, in accordance with the instructions of the Authority, for its Ofqual Recognition in respect of the TQ to be withdrawn;

15.5.2 the accumulated rights of the Authority are not affected;

15.5.3 the Authority grants to the Supplier a non-exclusive worldwide, royalty free irrevocable licence to use the IfATE Data solely to the extent that such IfATE Data consists of: (i) information relating to the identities of Providers and persons engaged by them, which it shall be entitled to use for any purpose; and (ii) Student Related Data provided that no individual Student can be identified from such Student Related Data, which it shall be entitled to use for research purposes in order to develop or improve upon any Supplier qualification (including material prepared, and training provided, in support of such qualification);

15.5.4 the Supplier must promptly return (or, where required by the Authority, delete) the IfATE Data except where required to retain copies by Law, the Conditions of Recognition, or for the purposes of exercising its rights under the licence granted under clause 15.4.3;

15.5.5 the Supplier must promptly return any of the Authority's property provided to it under this Contract;

15.5.6 the Supplier must at no cost to the Authority reasonably co-operate in the re-procurement and/or handover of the Services (including to a Replacement Supplier);

15.5.7 the Supplier must comply with the relevant provisions of Schedule 12 (*Exit Management*); and

15.5.8 this clause 15.4 and the following clauses survive the termination of this Contract: clauses 9, 12.3, 13, 16, 18, 19, 20, 22, 38 and 39 and any clauses and/or Schedules which are expressly or by implication intended to continue.

When the Supplier can end this Contract

15.6 The Supplier can terminate this Contract by issuing a Termination Notice if the Authority fails to pay any Charges which have fallen due under this Contract and which are directly payable by the Authority within 30 days of the date of a Reminder Notice issued by the Supplier in respect of such sum.

15.7 If the Supplier terminates this Contract under clause 15.5:

15.7.1 the Authority must promptly pay all outstanding Charges referred to in clause 15.5 to the Supplier; and

15.7.2 clauses 15.4.1 to 15.4.8 shall apply.

When Sub-Contracts can be ended

15.8 At the Authority's request, the Supplier must terminate (or procure the termination of (as the case may be)) any Sub-Contracts in any of the following events:

15.8.1 there is a change of Control of the relevant Subcontractor which is not pre-approved in writing by the Authority and which the Authority believes shall or may have an adverse impact on the Services;

15.8.2 the acts or omissions of the relevant Subcontractor have caused or materially contributed to a right of the Authority to terminate this Contract;

15.8.3 a Supplier Termination Event is caused or contributed to by the relevant Subcontractor or where any analogous events referred to in limbs (b), (d), (e), (f), (g), (h), (j) or (l) of the definition of Supplier Termination Event occurs in respect of the Subcontractor; or

15.8.4 the relevant Subcontractor sub-contracts any of its obligations in relation to the Services in breach of the requirements of this Contract.

16 How much each Party can be held responsible for

16.1 Subject to the following provisions of this clause 16 each Party's total aggregate liability under this Contract (whether in tort, contract or otherwise) for each claim or series of connected claims is no more than £1,000,000.

16.2 No Party is liable to the other for:

16.2.1 any indirect, special or consequential Loss; or

16.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect), provided always that, subject to clause 16.1, the Supplier acknowledges that the Authority may, amongst other things, recover from the Supplier the following Losses

incurred by the Authority, the Department and/or the ESFA, to the extent that they arise as a result of a Default by the Supplier:

(i) any additional operational and/or administrative costs and expenses, including costs relating to time spent by or on behalf of the Authority in dealing with the consequences of the Default;

(ii) any wasted expenditure or charges;

(iii) the additional cost of procuring Replacement Services for the remainder of the Contract Period, which shall include any incremental costs associated with such Replacement Services above those which would have been payable under this Contract;

(iv) any compensation or interest paid to a third party by the Authority; and

(v) any fine or penalty pursuant to Law and any costs in defending any proceedings which result in such fine or penalty.

16.3 The Authority does not give any warranty or undertaking as to the relevance, completeness, accuracy or fitness for purpose of any data information and/or documentation disclosed by or on behalf of the Authority prior to or after the Effective Date and neither the Authority nor any of its employees or agents shall be liable (howsoever arising) for any inaccuracy, omission, unfitness for purpose or inadequacy of any kind whatsoever in any such data information and/or documentation.

16.4 Nothing in this Contract shall operate to exclude or limit the liability of either Party in relation to the following:

16.4.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or subcontractors;

16.4.2 bribery or fraud or fraudulent misrepresentation by it or its employees; or

16.4.3 any liability that cannot be excluded or limited by Law.

16.5 Each Party must use its reasonable endeavours to mitigate any Losses which it suffers under or in connection with this Contract, including where any such Losses are covered by an indemnity.

16.6 When calculating the Supplier's liability under clause 16.1, Losses covered by Required Insurances will not be taken into consideration.

17 Insurance

17.1 Without prejudice to its obligations to the Authority under this Contract, including its indemnity obligations, the Supplier shall take out and maintain at its own cost, or procure the taking out and maintenance of, the Required Insurances. The Supplier shall ensure that each of the Required Insurances is effective no later than the date on which the relevant risk commences.

17.2 The Required Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.

17.3 The Required Insurances shall be taken out and maintained with insurers who are: (a) of good financial standing; (b) appropriately regulated; and (c) of good repute in the international insurance market.

17.4 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Required Insurances.

17.5 Where the Supplier has failed to purchase any of the Required Insurances or maintain any of the Required Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Required Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

17.6 The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Required Insurances, provide evidence, in a form satisfactory to the Authority, that the Required Insurances are in full force and effect and meet in full the requirements of this clause 17. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Contract.

17.7 The Supplier shall ensure that the public and products liability policy forming part of the Required Insurances shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Services and for which the Supplier is legally liable.

18 Data protection and information

18.1 Each Party shall comply with the Data Protection Legislation.

18.2 The Supplier must ensure that Personal Data is Processed in accordance with Schedule 9 (*Data Handling and Security Management*).

18.3 The Supplier must not remove any ownership or security notices in or relating to the IfATE Data.

18.4 The Supplier must make accessible back-ups of all IfATE Data, stored in an agreed off-site location. The Supplier must send the Authority copies every six Months of the Ancillary Materials and the Key Materials (in each case to the extent that these have not already been provided to the Authority), and any further information falling within the definition of IfATE Data as may be requested by the Authority in writing from time to time.

18.5 The Supplier must ensure that any Supplier system holding any IfATE Data, including back-up data, is a secure system that complies with the Security Policy and the relevant provisions of Schedule 9 (*Data Handling and Security Management*).

18.6 If at any time the Supplier suspects or has reason to believe that the IfATE Data provided or generated under this Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Authority and immediately suggest remedial action.

18.7 If the IfATE Data is corrupted, lost or sufficiently degraded so as to be unusable the Authority may either or both:

18.7.1 tell the Supplier to restore or get restored IfATE Data as soon as practical but no later than 5 Working Days from the date that the Authority receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or

18.7.2 restore the IfATE Data itself or using a third party.

18.8 The Supplier must pay each Party's reasonable costs of complying with clause 18.7 unless the Authority is at fault.

18.9 The Supplier:

18.9.1 must provide the Authority with all IfATE Data in an agreed open format within 10 Working Days of a written request;

18.9.2 must have documented processes to guarantee prompt availability of IfATE Data if the Supplier stops trading;

18.9.3 must securely destroy all Storage Media that has held IfATE Data at the end of life of that media using Good Industry Practice;

18.9.4 must securely erase all IfATE Data and any copies it holds when asked to do so by the Authority unless required by Law to retain it; and

18.9.5 indemnifies the Authority against any and all Losses suffered or incurred by the Authority if the Supplier and/or any Key Subcontractor breaches this clause 18 and/or any Data Protection Legislation.

19 What must be kept confidential

Confidential Information

19.1 Each Party must, subject to the following provisions of this clause 19;

19.1.1 keep all Confidential Information it receives confidential and secure;

19.1.2 not disclose, use or exploit the Confidential Information disclosed by the Disclosing Party without the Disclosing Party's prior written consent, except for the purposes anticipated under this Contract; and

19.1.3 immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

19.2 Notwithstanding clause 19.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

19.2.1 where disclosure is required by applicable Law or by a court with the required jurisdiction, if the Recipient Party (to the extent that it is permitted

to do so by such applicable Law or by such court) notifies the Disclosing Party in advance of disclosure of the full circumstances, the affected Confidential Information and extent of the disclosure;

19.2.2 if the Recipient Party already had the information without obligation of confidentiality before it was disclosed to it by the Disclosing Party;

19.2.3 if the information was given to it by a third party without obligation of confidentiality;

19.2.4 if the information was in the public domain at the time of the disclosure;

19.2.5 if the information was independently developed without access to the Confidential Information of the Disclosing Party;

19.2.6 to its auditors or for the purposes of regulatory requirements;

19.2.7 on a confidential basis, to its professional advisers on a need-to-know basis;

19.2.8 to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010; and/or

19.2.9 where disclosure is permitted in accordance with Schedule 4 (*Co-operation*).

19.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under this Contract. The Supplier must ensure that the Supplier Staff enter into a direct confidentiality agreement with the Authority at the Authority's request.

19.4 The Authority may disclose Confidential Information in any of the following cases:

19.4.1 on a confidential basis to the employees, agents, consultants and contractors of the Authority;

19.4.2 on a confidential basis to any Crown Body, any successor body to a Crown Body or any company that the Authority transfers or proposes to transfer all or any part of its business to;

19.4.3 where permitted by the Apprenticeships, Skills, Children and Learning Act 2009, (including to the Department, ESFA or Ofqual and as contemplated by clause 5.15 (*Developing the TQ and achieving IfATE Approval*);

19.4.4 if the Authority (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;

19.4.5 where requested by Parliament;

19.4.6 under clauses 4.10 (*Pricing and payments*) and 20 (*When information can be shared*); or

19.4.7 save for Exit Information, where the information was generated as part of the provision of the Services.

19.5 For the purposes of clauses 19.2 to 19.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in this clause 19.

Student Related Data

19.6 The Supplier must:

19.6.1 keep all Student Related Data confidential and secure;

19.6.2 immediately notify the Authority if it suspects unauthorised access, copying, use or disclosure of the Student Related Data.

19.7 The Supplier shall not store, copy, disclose, or use the Student Related Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

Transparency Information and other disclosures

19.8 Transparency Information and any information which is exempt from disclosure by clause 20 (*When information can be shared*) is not Confidential Information.

19.9 The Supplier must not make any press announcement or publicise this Contract or the output of the Services (including the Student Related Data) without the prior written consent of the Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

20 When information can be shared

20.1 The Supplier acknowledges that:

20.1.1 the Transparency Reports; and

20.1.2 the content of this Contract, including any changes to this Contract agreed during the Term, except for (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Authority; and (ii) Commercially Sensitive Information,

(together the "**Transparency Information**") is not Confidential Information.

20.2 The Supplier must tell the Authority within 48 hours if it receives a Request For Information.

20.3 Within the timescales required by the Authority, the Supplier must give the Authority full co-operation and information needed so the Authority can:

20.3.1 publish the Transparency Information; and

20.3.2 comply with any Request for Information.

20.4 The Supplier acknowledges that the Authority may be required under the FOIA and EIRs to disclose information (including Confidential Information and Commercially Sensitive Information) without consulting or obtaining consent from the Supplier. However, to the extent that it is permitted to do so (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA), the Authority shall, in relation to any Request for Information relating to Confidential Information or Commercially Sensitive Information of the Supplier:

20.4.1 notify the Supplier of such Request for Information as soon as is reasonably practicable; and

20.4.2 allow the Supplier to make representations in relation to any exemptions the Supplier considers may apply to the disclosure of its information under the Request for Information and take such representations into account when making its decision of what it will disclose.

20.5 Notwithstanding any other provision in this Contract, the Authority shall be responsible for determining in its absolute discretion whether any Commercially Sensitive Information and/or any other information is exempt from disclosure in accordance with the FOIA and/or the EIRs.

21 Invalid parts of this Contract

If any part of this Contract is held to be void or otherwise unenforceable by any court of competent jurisdiction, such part shall to the extent necessary to ensure that the remaining provisions of this Contract are not void or unenforceable be deemed to be deleted and the validity and/or enforceability of the remaining provisions of this Contract shall not be affected.

22 No other terms apply

The provisions incorporated into this Contract are the entire agreement between the Parties. This Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

23 Other people's rights in this Contract

23.1 The Department may enforce any of the Authority's rights under this Contract in relation to which the Department is to benefit. The Department's consent is not required to amend this Contract.

23.2 Save as provided in clause 23.1 or expressly stated in this Contract, no third parties shall be entitled to enforce any term of this Contract.

24 Circumstances beyond either Party's control

24.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under this Contract while the inability to perform continues, if it both:

24.1.1 provides a Force Majeure Notice to the other Party; and

24.1.2 uses all reasonable measures to reduce the impact of the Force Majeure Event.

24.2 The Authority can terminate this Contract if the provision of the Services is materially affected by a Force Majeure Event which lasts for 90 days continuously.

24.3 Where the Authority terminates under clause 24.2:

24.3.1 each Party must cover its own Losses; and

24.3.2 subject to clause 24.3.1, clause 15.4 applies.

24.4 Neither Party can rely on clause 24.1 where the inability to perform its obligations arises, directing or indirectly, due to the exit from the European Union by the United Kingdom.

24.5 The Supplier may not rely on clause 24.1 to the extent that the inability to perform its obligations arises directly or indirectly out of a failure by the Supplier to comply with its Business Continuity Plan.

25 Relationships created by this Contract

25.1 This Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent itself accordingly and ensure the Supplier Staff do so.

26 Giving up contract rights

26.1 A partial or full waiver or relaxation of the terms of this Contract by one Party is only valid if it is stated to be a waiver in writing to the other Party.

27 Transferring responsibilities

27.1 The Supplier must not assign, transfer or otherwise dispose of its rights, obligations and/or liabilities under the whole or any part of this Contract without Approval.

27.2 The Authority can assign, novate or transfer this Contract or any part of it to any Crown Body, public sector body or private sector body which performs the functions of the Authority.

27.3 The Supplier must enter into a novation agreement in the form that the Authority specifies where the Authority wishes to exercise its rights under clause 27.2.

27.4 The Supplier can terminate this Contract novated under clause 27.2 to a private sector body where an Insolvency Event occurs in respect of that private sector body.

27.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

28 Changing this Contract

28.1 If any change is required which is an Inclusive TQ Change, clause 8 (*TQ Changes*) shall apply in relation to such change, and this clause 28 shall not apply to any Inclusive TQ Change.

28.2 Either Party can request a Variation to this Contract, including the addition or removal of one or more Occupational Specialist Components.

28.3 The Supplier cannot unreasonably withhold or delay their consent to a Variation to this Contract.

28.4 The Supplier must provide an Impact Assessment either:

28.4.1 with the Variation Form, where the Supplier requests the Variation; or

28.4.2 within the time limits included in a Variation Form where the Authority requests the Variation.

28.5 If the Variation cannot be agreed or resolved by the Parties, the Authority can either:

28.5.1 agree that this Contract continues without the Variation; or

28.5.2 treat such failure as a Dispute which shall be addressed through the Dispute Resolution Procedure.

28.6 A Variation of this Contract is only effective if agreed in writing and signed by both Parties.

28.7 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Charges and/or the Fees in respect of that change.

28.8 If there is a Specific Change in Law or one is likely to happen during the Contract Period, the Supplier must give the Authority notice of the likely effects of the Specific Change in Law as soon as reasonably practical. The Supplier must also say if it thinks any Variation is needed either to the Services, the Products and/or this Contract and provide evidence:

28.8.1 that the Supplier has kept costs as low as possible and/or maximised any cost savings (as the case may be) including any Subcontractor costs; and

28.8.2 of how it has affected or will affect the Supplier's costs and/or those of any Subcontractor.

28.9 Any Variation because of a Specific Change in Law must be implemented using clauses 28.1 to 28.6.

28.10 If another awarding organisation has a contract with the Authority for the provision of services similar to the Services to deliver a different technical qualification as part of the T Levels Programme and that other awarding organisation suffers a Supplier Termination Event following which its contract with the Authority is terminated or the relevant contract is otherwise lawfully terminated, the Supplier agrees that the Authority shall have the option to request that the Supplier takes over the delivery of that different technical qualification and any related services as a Variation, which will be implemented using clauses 28.1 to 28.6. The Charges and Fees relating to such a Variation shall be agreed between the Parties as part of the Impact Assessment for the relevant Variation, each Party acting reasonably and promptly, prior to the Supplier commencing work on the Variation. The relevant Charges and Fees shall:

28.10.1 be a reasonable cost for implementing the Variation in the circumstances;

28.10.2 take into account the charges and fees that the other awarding organisation was charging in relation to that different technical qualification prior to suffering the Supplier Termination Event; and

28.10.3 take into account and be calculated using:

(i) for personnel related costs and other relevant charges which are set out in the Rate Card, the applicable Rate Card rates; and

(ii) reasonable charges for any non-personnel related costs which are not included in the Rate Card and which will be incurred by the Supplier to implement the Variation; and

(iii) the same basis and the same logic used by the Supplier to determine the relevant costs, Charges and Fees for the Services.

29 How to communicate about this Contract

29.1 All notices under this Contract must be in writing and are considered effective on the Working Day of delivery as long as delivered before 5:00 pm on a Working Day. Otherwise the notice is effective on the next Working Day. Unless expressly stated in this Contract or otherwise communicated in writing by the Authority, an email is not effective notice unless also sent by post or delivered by hand on the same day. For the avoidance of doubt, this clause 29.1 does not apply to a Variation, which must be implemented in accordance with clauses 28.2 to 28.6.

29.2 Subject to clause 29.1, notices to the Authority must be sent to the Authority Authorised Representative's address and email address, and all notices must be copied to the Authority's Head of Commercial Delivery Management [redacted] and the Authority's Head of Legal [redacted]

29.3 Subject to clause 29.1, notices to the Supplier must be sent to the Supplier Authorised Representative's address and email address.

29.4 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

30 Dealing with claims

30.1 If a Beneficiary is notified of or otherwise becomes aware of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days after such notification or date of first awareness.

30.2 At the Indemnifier's cost the Beneficiary must both:

30.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and

30.2.2 give the Indemnifier reasonable assistance with the Claim if requested.

30.3 The Beneficiary must not make admissions about the Claim or enter into any agreement or compromise in relation to the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

30.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary's reputation (or, in the case of the Authority as a Beneficiary, the reputation of the Authority, the Department and/or the ESFA or the wider T Levels Programme).

30.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

30.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

30.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the relevant Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

30.7.1 the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or

30.7.2 the amount the Indemnifier paid the Beneficiary for the Claim.

31 <u>Preventing fraud, bribery and corruption</u>

31.1 The Supplier must not during the Term:

31.1.1 commit a Prohibited Act or any other criminal offence in regulations 38(8), 38(9) and/or 38(10) of the Regulations; and/or

31.1.2 do or allow anything which would cause the Authority, including any of its employees, consultants, contractors, subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

31.2 The Supplier must during the Term:

31.2.1 create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same;

31.2.2 keep full records to show it has complied with its obligations under this clause 31 and give copies to the Authority on request; and

31.2.3 if required by the Authority, within 20 Working Days of the Effective Date, and then annually, certify in writing to the Authority, that it has complied with this clause 31, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

31.3 The Supplier must immediately notify the Authority if it becomes aware of any breach of clauses 31.1 or 31.2, or has any reason to think that it, or any of the Supplier Staff, has either:

31.3.1 been investigated or prosecuted for an alleged Prohibited Act;

31.3.2 been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any Crown Body;

31.3.3 received a request or demand for any undue financial or other advantage of any kind related to this Contract; or

31.3.4 suspected that any person or Party directly or indirectly related to this Contract has committed or attempted to commit a Prohibited Act.

31.4 If the Supplier notifies the Authority as required by clause 31.3, the Supplier must respond promptly to the Authority's further enquiries, co-operate with any investigation and allow the Audit of any relevant books, records and documentation.

31.5 In any notice the Supplier gives under clause 31.4 it must specify the:

31.5.1 Prohibited Act;

31.5.2 identity of the party who it thinks has committed the Prohibited Act; and

31.5.3 action it has decided to take.

32 Equality, diversity, human rights and modern slavery

32.1 The Supplier must perform its obligations under this Contract (including those in relation to the Services), in accordance with:

32.1.1 all applicable equality Law (whether in relation to race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise); and

32.1.2 any other requirements and instructions which the Authority reasonably imposes related to equality Law.

32.2 The Supplier must perform its obligations under this Contract (including those in relation to the Services) giving consideration to the Authority's Equity, Diversity and Inclusion toolkit as published on the Authority's website or provided to the Supplier from time to time.

32.3 The Supplier must take all necessary steps, and inform the Authority of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on this Contract.

32.4 The Supplier must use Good Industry Practice to ensure that there is no slavery or human trafficking in its supply chains and must notify the Authority immediately if it becomes aware of any actual or suspected incidents of slavery or human trafficking in its supply chains.

32.5 The Supplier must at all times conduct its business in a manner that is consistent with any anti-slavery policy of the Authority and shall provide to the Authority any reports or other information that the Authority may request as evidence of the Supplier's compliance with this clause 32.4 and/or as may be requested or otherwise required by the Authority in accordance with any Authority anti-slavery policy.

33 Health and safety

33.1 The Supplier must perform its obligations meeting the requirements of:

33.1.1 all applicable Law regarding health and safety;

33.1.2 the Authority's current health and safety policy, as provided to the Supplier, to the extent that Supplier Staff are located at any Authority premises in the course of performing the Services under this Contract.

34 Environment

34.1 The Supplier must ensure that Supplier Staff are aware of and comply with the Environmental Policy.

35 Tax

35.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines.

35.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under this Contract, the Supplier must both:

35.2.1 comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and

35.2.2 indemnify the Authority against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Services by the Supplier or any Supplier Staff.

36 Conflict of interest

36.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

36.2 The Supplier must promptly notify and provide details to the Authority if a Conflict of Interest happens or is expected to happen.

36.3 The Authority can terminate this Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

37 Reporting a breach of this Contract

37.1 As soon as it is aware of it, the Supplier and Supplier Staff must report to the Authority any actual or suspected breach of:

37.1.1 Law; or

37.1.2 clauses 31 to 36 (inclusive).

37.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith report a breach listed in clause 37.1 to the Authority or a Prescribed Person.

38 Resolving disputes

38.1 If there is a Dispute, nominated senior representatives of each Party who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

38.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using clauses 38.3 to 38.5.

38.3 Unless the Authority refers the Dispute to arbitration using clause 38.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

38.3.1 determine the Dispute; and/or

38.3.2 grant interim remedies, or any other provisional or protective relief.

38.4 The Supplier agrees that the Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

38.5 The Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 38.3, unless the

Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 38.4.

38.6 The Supplier cannot suspend the performance of this Contract during any Dispute.

38.7 To the extent that a Dispute relates to whether or not the Supplier has complied with a Condition of Recognition and/or requirement of Ofqual Recognition, the Parties agree that they shall request that Ofqual shall make the final decision as to whether the requirements of that Condition of Recognition and/or Ofqual Recognition have been met and any such decision by Ofqual shall be binding on both Parties.

39 Which law applies

This Contract and any issues arising out of, or connected to it, are governed by English law.

Signed by

PEARSON EDUCATION LTD

[redacted]

Signed by

THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION

[redacted]

Schedule 1

Definitions and Interpretation

1 Interpretation

1.1 In this Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Schedule 1 (*Definitions and Interpretation*) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In this Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 references to a legal entity (other than the Supplier) shall include unless otherwise expressly stated any statutory successor to such entity and/or the relevant functions of such entity, and references to the Department shall include, where relevant, the ESFA;

1.3.5 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.6 any reference to this Contract or to any other document shall include any variation, amendment or supplement to such document;

1.3.7 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.8 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.9 references to "**clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses of and schedules to the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.10 references to "**paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and

1.3.11 the headings in this Contract are for ease of reference only and shall not affect the interpretation or construction of this Contract.

2 Definitions

2.1 In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

"**Academic Year**" means 1 August to 31 July in the following calendar year;

"**Additional Service**" means each additional service listed in Schedule 6 (Pricing Schedule) and detailed in Annex 10 to the Service Requirements;

"**Affected Party**" means the party seeking to claim relief in respect of a Force Majeure Event;

"**Affiliates**" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

"**Ancillary Materials**" means all information and materials (other than Key Materials) to which the Authority and/or a Future Supplier would require access for use for the Portability Purposes, and any other materials which would be required on or to facilitate succession to a Future Supplier in a seamless manner in relation to the TQ offered or Operated by the Supplier. Ancillary Materials shall include, without limitation:

(a) Student results including grades;

(b) statistical analysis for grading (excludes the systems supporting the analysis);

(c) lists of Providers;

(d) marked Student evidence (with moderation outcomes);

(e) documentation which provides an overview or analysis of Student performance (including chief examiner and chief moderator reports), which include but are not limited to, examples of student responses to assessment questions and/or tasks as well as narrative explaining why students did well/ less well on individual items/ components/ subcomponents);

(f) data on Student credits;

g) data on Student appeals;

(h) data on special considerations for Students;

(i) the Assessment Strategy;

(j) Student registrations;

(k) draft materials in preparation for forthcoming assessments;

(l) the Key Dates Schedule (in respect of forthcoming assessments);

(m) lists, with contact details, of people contracted by the Supplier to perform or oversee activities which are necessary for the conduct and quality assurance of assessments for the TQ;

(n) materials from completed assessments, such as completed Students' examination answer booklets; and

(o) TQ Live Assessment Materials

"**Approval**" means the prior written consent of the Authority and "Approve" and "Approved" shall be construed accordingly;

"**Approved Assessment Strategy**" shall have the meaning given in Schedule 2 (Service Requirements);

"**Approved Initial TQ Deliverables**" means the Initial TQ Deliverables approved by the Authority in accordance with clause 5.13 (Developing the TQ and achieving IfATE Approval) or clause 8.10 or 8.11 (TQ Changes) (as the case may be) as such deliverables are reviewed and updated in accordance with this Contract;

"**Approved Provider**" means an Eligible Provider that has been granted Provider Approval in accordance with clause 7.1 (Interaction with Providers) and in respect of which such Provider Approval has not been revoked pursuant to clause 7.2 (Interaction with Providers);

"**Approved Provider's Quality Assurance Process**" means the quality assurance process referred to in, and meeting the requirements of, the relevant part of the Product Description for the TQ Specification;

"**Approved TQ Specification**" means the TQ Specification approved by the Authority in accordance with clause 5.13 (Developing the TQ and achieving IfATE Approval) or clause 8.10 or 8.11 (TQ Changes) (as the case may be);

"**Assessment Strategy**" means the assessment strategy referred to in, and meeting the requirements of, the Product Description for the Assessment Strategy, which unless otherwise agreed in writing with the Authority must be consistent with the relevant details forming part of the Supplier's Response;

"**Assessors**" means any assessor appointed by the Supplier to assess performance by Students in respect of the TQ Live Assessment Materials;

"**Audit**" means the Authority's right to:

(a) verify the accuracy of the Charges and any other amounts payable by the Authority (including proposed or actual variations to them in accordance with this Contract);

(b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services (including the supply of the Products);

(c) verify the Supplier's and each Subcontractor's compliance with the applicable Law;

(d) identify or investigate actual or suspected breach of clauses 31 to **Error! Unknown switch argument.**, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;

(e) verify the Supplier's compliance with Schedule 9 (*Data Handling and Security Management*);

(f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, or their ability to provide the Services including to supply the Products;

(g) obtain such information as is necessary to fulfil the Authority's obligations to supply information for Parliamentary, ministerial, judicial or administrative

purposes including the supply of information to the Comptroller and Auditor General;

(h) review any books of account and the internal contract management accounts kept by the Supplier in connection with this Contract;

(i) carry out the Authority's internal and statutory audits and to prepare, examine and/or certify the Authority's annual and interim reports and accounts;

(j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(k) verify the accuracy and completeness of any Management Information delivered or required by this Contract; and/or

(l) obtain such information as is necessary to undertake a review and/or assessment of the performance of the whole or any part of the T Levels Programme;

"Auditor" means any, or any combination, of:

(a) the Authority's internal and external auditors;

(b) the Authority's statutory or regulatory auditors;

(c) the Comptroller and Auditor General, its staff and/or any appointed representatives of the National Audit Office;

(d) HM Treasury or the Cabinet Office;

(e) any party formally appointed by the Authority to carry out audit or similar review functions; and

(f) successors or assigns of any of the above;

"Authority Authorised Representative" means the person referred to in Schedule 20 as such or the representative appointed by the Authority from time to time in relation to this Contract as notified in writing (which may, in the case of this specific notification, be by email only) to the Supplier;

"Authority Procedural Review" means the Authority's procedural review process as published on the Authority's web site from time to time;

"Awarding Organisation" means a body recognised by Ofqual as a provider of certain qualifications;

"Background IPR" means any IPR owned by a party prior to the Effective Date or created or developed by a party independently of this Contract, but does not include IPR in Key Materials;

"Beneficiary" means a Party having (or claiming to have) the benefit of an indemnity under this Contract;

"Breach of Security" means the occurrence of:

(g) any unauthorised access to or use of the Services and/or the Products, the sites from which the Services are delivered (and/or where the Products are developed, and/or stored) and/or any information and communication technology, information or data (including the Confidential Information and the IfATE Data) used by the Authority and/or the Supplier in connection with this Contract; and/or

(h) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the IfATE Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Contract,

in either case as may be more particularly set out in the Security Policy;

"Business Continuity Plan" means the business continuity and disaster recovery plan relating to this Contract, as set out in Schedule 10 (Business Continuity);

"Cabinet Office Statement" means the Cabinet Office Statement of Practice – Staff Transfers in the Public Sector 2000 (as revised 2013) as may be amended or replaced;

"Change in Law" means any change in Law which impacts on the provision of the Services (including the supply of the Products) and/or the performance of this Contract which comes into force after the Effective Date;

"Charges" means:

(a) the Development Charge payable to the Supplier by the Authority in accordance with clause 4.1.1 (*Pricing and payments*);

(b) in respect of any Exclusive TQ Change, the amount (exclusive of any applicable VAT) agreed or determined in respect of such Exclusive TQ Change in accordance with clause 8.6 (*TQ Changes*); and

(c) in respect of any other Variation, the amount agreed pursuant to clause 28 (*Changing this Contract*) in respect of such Variation;

"Claim" means any claim for which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;

"Cohort" means a group of Students who are registered by an Approved Provider with the Supplier to commence the TQ in the relevant Academic Year;

"Commercially Sensitive Information" means the Confidential Information listed in Schedule 18 (*Commercially Sensitive Information*) comprising of commercially sensitive information relating to the Supplier, its IPR or its business which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;

"**Comparable Supply**" means the supply of services to the Authority or another customer or client of the Supplier that are the same as or similar to the Services (including the supply of products that are the same as or similar to the Products) including services relating to qualifications in England outside the T Levels Programme;

"**Conditions of Recognition**" means the conditions of Ofqual Recognition imposed on the Supplier by Ofqual including any general level conditions, qualification level conditions, subject level conditions and special conditions;

"**Confidential Information**" means, subject to clause 19.8 (*What must be kept confidential*), any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of the Authority or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "**confidential**") or which ought reasonably to be considered to be confidential. Confidential Information shall not include Student Related Data;

"**Conflict of Interest**" means a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Authority under this Contract, in the reasonable opinion of the Authority. This includes where:

(a) the Supplier's interests in any activity undertaken by the Supplier, on its behalf, or by an Affiliate of the Supplier have the potential to lead the Supplier to act contrary to the Supplier's interests in the development, delivery and award of the TQ in accordance with the Conditions of Recognition;

(b) a person who is connected to the development, delivery or award of the TQ by the Supplier has interests in any other activity which have the potential to lead that

person to act contrary to his or her interests in that development, delivery or award in accordance with the Conditions of Recognition; or

(c) an informed and reasonable observer would conclude that either of these situations was the case;

"**Continuing Activities**" means activities of the Supplier under this Contract in relation to the TQ which continue following the end of the second Academic Year for the final Exclusive Cohort, such as retakes, appeals, and ongoing records management;

"**Contract**" means this contract;

"**Contract Month"** means each calendar month, provided that:

(a) the first Contract Month shall commence on and from the Effective Date and shall end on the last day of the calendar month in which the Effective Date occurs; and

(b) the last Contract Month shall commence on and from the first day of the calendar month in which the End Date occurs and shall end on the End Date;

"Contract Period" means the period for which this Contract would remain in force (taking into account any current Extension Period) if not terminated earlier;

"Control" means the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and/or policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controlled" shall be construed accordingly;

"Controller" has the same meaning as in the GDPR;

"Core Terms" means the terms set out in the main body of this Contract;

"Critical Service Failure" means:

(a) the Ofqual Recognition of the Supplier to make the TQ available to Approved Providers for delivery to Students is withdrawn;

(b) a failure by the Supplier to make the Final Submission by the Final Approval Milestone Date or the failure of any Final Submission (or Final Re-Submission) to meet the requirements necessary to achieve IfATE Approval (in each case other than where such failure results from a breach of this Contract by the Authority);

(c) a failure by the Supplier to make a Final Re-Submission within the time period required by clause 5.13.2(*Developing the TQ and achieving IfATE Approval*) (other than where such failure results from a breach of this Contract by the Authority);

(d) the Authority withdraws IfATE Approval (having previously awarded IfATE Approval) in accordance with this Contract;

(e) any failure by the Supplier to perform a Designated Action within the specified timeframe for that Designated Action (other than where such failure results from a breach of this Contract by the Authority);

(f) any Supplier Termination Event which has occurred in respect of the Supplier in its role as an Awarding Organisation for any part of the T Levels Programme outside this Contract;

(g) any Breach of Security which either (i) results in material personal data being lost or compromised or shared without authorisation; or (ii) is not notified to the Authority promptly (and in any event within one Working Day);

(h) the Supplier breaches its obligations relating to the confidentiality of assessment papers (prior to the relevant assessment date) and/or Student results (prior to the relevant publication date); and

(i) any other event, matter or circumstance which is expressed to be (or deemed to be) a Critical Service Failure in this Contract;

"Crown Body" means the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including government ministers and government departments and bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;

"Data Protection Legislation" means:

(a) the GDPR;

(b) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and

(c) all applicable Law about the processing of personal data and privacy;

"Default" means any breach of the obligations of the Supplier (including abandonment of this Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of this Contract and in respect of which the Supplier is liable to the Authority;

"Deliverable" means all information and data the Supplier creates, identifies for use, or uses as part of or for the Operation of the TQ, including Products and Management Information;

"Department" means the Secretary of State for Education;

"Designated Action" means an action which the Authority requires the Supplier to take within a specified timeframe to obtain and/or maintain IfATE Approval and/or to ensure ongoing compliance of the Supplier with the terms of this Contract and such action may include:

(a) working in a prescribed way with Authority personnel and/or a third party appointed by the Authority to achieve certain specified performance and/or progress improvements;

(b) taking appropriate remedial actions in the event that any Initial Development Services and/or interim Products provided during the Development Phase are not in line with the trajectory set out in the Implementation and Delivery Plan;

(c) temporarily suspending and/or restricting any elements (in full or part) of the Services (including the supply of any Products);

(d) complying with increased performance monitoring, provision of information and/or increased audit;

(e) complying with any reasonable instructions of the Authority to help to mitigate actual and/or potential risks associated with delivery of the T Levels Programme; and/or

(f) providing reasonable cooperation to other Awarding Organisations and third party suppliers of the Authority appointed in connection with the T Levels Programme;

"Development Charge" means the amount (exclusive of any applicable VAT) referred to as the "Qualification development charge" in Schedule 6 (Pricing Schedule);

"Development Phase" – The period between commencement of the Contract and the Approval of the TQ, being the period during which the TQ is developed by the Supplier.

"Development Phase Report" means the report referred to in the second row of the first column in the Table in Annex 9 to the Service Requirements and containing the information set out in the second row of the second column of that Table;

"Devolved Administration" means the government of Scotland, Northern Ireland and/or Wales;

"Disclosing Party" means the Party directly or indirectly providing Confidential Information to the other Party in accordance with clause 19 (What must be kept confidential);

"Dispute" means any claim, dispute or difference which arises out of or in connection with this Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of this Contract, whether the alleged liability shall arise under English law or

under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;

"Dispute Resolution Procedure" means the dispute resolution procedure set out in clause 38 (Resolving disputes);

"Documentation" means descriptions of the Services (including the Products) and KPIs, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) that is required to be supplied by the Supplier to the Authority under this Contract as:

(d) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Authority to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that are utilised to supply the Services or Products;

(e) is required by the Supplier in order to supply the Services or Products; and/or

(f) has been or shall be generated for the purpose of supplying the Services or Products;

"Early Exit" means any termination of this Contract that occurs prior to the Supplier achieving IfATE Approval;

"Effective Date" means the date on which the last Party to sign has signed this Contract;

"Effective Date of Variation" means the date on which the Variation Form comes into effect;

"EIRs" means the Environmental Information Regulations 2004;

"Eligible Provider" means any Provider referred to in the list referenced in Part 1 of Annex 8 to the Service Requirements in respect of the relevant Cohort, as such list may be updated from time to time by the Authority, or notified in writing to the Supplier in accordance with Part 2 of Annex 8 to the Service Requirements;

"Emergency Exit" means any termination of this Contract other than an Early Exit that is a:

(g) termination of the whole or part of this Contract prior to the Expiry Date (as extended by any Extension Period); or

(h) wrongful termination or repudiation of this Contract by either Party;

“Employee Liability” means all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:

(i) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;

(j) unfair, wrongful or constructive dismissal compensation;

(k) a failure to comply with TUPE;

(l) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;

(m) compensation for less favourable treatment of part-time workers or fixed term employees;

(n) outstanding debts and unlawful deduction of wages including any PAYE and National Insurance in relation to payments made by the Authority or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Subcontractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions;

(o) claims whether in tort, contract or statute or otherwise;

(p) any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;

“Employer” means any employer who has or is likely to employ Students who have successfully obtained a T Level qualification;

“Employer and Provider Engagement Strategy” means a clear and detailed strategy detailing the approach to engaging with Employers and Providers in relation to the design, development, delivery, validation and update of the TQ and the Services, including the approach to sharing early and/or amended drafts of the Initial TQ Deliverables and TQ Deliverables with Employers and Providers (as applicable);

"Employer Set Project Grade Exemplar Responses" means actual marked examples of Students' assessment evidence, selected after awarding, as referred to in Service

Requirement 5.1, which; meet the requirements for grade A and grade E; are produced (and reviewed each Academic Year) in consultation with Employers; and are accompanied by an explanatory commentary;

"Employer Set Project Guide Exemplar Responses" means indicative guide examples of Students' assessment evidence as referred to in Service Requirement 5.1, which; the Supplier judges would be likely to meet the minimum requirements for grade A and grade E; are produced in consultation with Employers; and are accompanied by an explanatory commentary;

"End Date" means the earlier of:

(a) the Expiry Date (as extended by any Extension Period implemented by the Authority under clause 15 (*Ending or extending this Contract*) or as reduced by the Authority in accordance with clause 14.3.2 (*What may happen if there are issues with your provision of the Services*); or

(b) if this Contract is terminated before the date specified in (a) above, the date of termination of this Contract;

"Enhanced Entry Fee" shall have the meaning given in paragraph 2.3 of Schedule 6A (Adaptive Pricing);

"Entry Fee" shall have the meaning as referred to at subsection (a) of the definition of Fees;

"Entry Transition Period" means the period from the Effective Date of this Contract to the End Date of the Authority's Contract with the Former Supplier, eg from the point when the Supplier has been awarded a contract for provision of the TQ, but a contract with the Former Supplier remains in place for existing Students;

"Entry Transition Plan" means the plan produced as part of the Supplier's Tender, and included in Schedule 5 (Supplier's Response), where relevant, and updated by the Supplier as contemplated by Schedule 4 (Co-Operation);

"Environmental Policy" means to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Authority;

"Equality and Human Rights Commission" means the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;

"ESFA" means the Education and Skills Funding Agency;

"Exclusive Cohort" has the meaning given in clause 2.2 (*Appointment and exclusivity*);

"**Exclusive TQ Change**" means:

(a) the addition of one or more new Occupational Specialist Component(s) which are to be added to the TQ following the Initial Content Date; and/or

(b) the removal of one or more Occupational Specialist Component(s); and/or

(c) a TQ Change which is requested by the Authority as a result of revision to a relevant Standard arising out of a statutory review of such Standard by the Authority under section A2D3 of the Apprenticeships, Skills, Children and Learning Act 2009;

"**Exemplification Materials"** means the Guide Standard Exemplification Materials and the Grade Standard Exemplification Materials;

"Exit Information" has the meaning given to it in paragraph 3.2 of Schedule 12 (*Exit Management*);

"Exit Plan" means the plan produced and updated by the Supplier during the Term in accordance with paragraphs 1 and 2 of Schedule 12 (*Exit Management*);

"Expiry Date" means 2 years following expiry of the final Academic Year for the final Exclusive Cohort;

"Extension Entry Fee" shall have the meaning given in paragraph 3.1.2 of Schedule 6A (Adaptive Pricing);

"Extension Period" means a period equal to that required to provide the Services (including the supply of any Products) to extend the contract –

(a) for one further Cohort, such period to commence at the start of the Academic Year immediately following the end of the Academic Year in which the fifth Exclusive Cohort commences the TQ; and, at the Authority's discretion;

(b) for a second further Cohort, such period to commence at the start of the Academic Year immediately following the end of the Academic Year in which the sixth Exclusive Cohort commences the TQ; and at the Authority's discretion;

(c) for a third further Cohort, such a period to commence at the start of the Academic Year immediately following the end of the Academic Year in which the seventh Exclusive Cohort commences the TQ;

"Extension Review" shall have the meaning given in paragraph 1.1.2 of Schedule 6A (Adaptive Pricing);

"**Fees**" means:

(a) in respect of the provision of the Provider Services (other than the Additional Services), the amount (exclusive of any applicable VAT) referred to as "Entry fee" in Schedule 6 (*Pricing Schedule*) payable per registered Student to the Supplier by the Approved Providers in accordance with clause 4.1.2 (*Pricing and payments*); and

(b) the Additional Services, the amount (exclusive of any applicable VAT) applicable to the relevant Additional Service as set against that Additional Service in Schedule 6 (*Pricing Schedule*) payable to the Supplier by the Approved Providers in accordance with clause 4.1.2 (*Pricing and payments*);

(c) in each case, as such fees are adjusted in accordance with clauses 4.12 and 4.13 (*Pricing and payments*);

"First Extension" shall have the meaning given in paragraph 3.1 of Schedule 6A (Adaptive Pricing);

"Final Approval Milestone" means the Milestone set out in the third row of the Table in Annex 7 to the Service Requirements;

"Final Approval Milestone Date" means the date set out against the Final Approval Milestone in the second column of the Table at Annex 7 to the Service Requirements;

"Final Milestone Payment" means an amount equal to 30% of the Development Charge;

"Final Re-Submission" means the relevant documentation and/or additional information that the Supplier is required to re-submit in accordance with clause 5.13.2 (*Developing the TQ and achieving IfATE Approval*);

"Final Submission" means the Submission applicable to the Final Approval Milestone;

"Final Updated Projection" shall have the meaning given in paragraph 3.1.1 of Schedule 6A (Adaptive Pricing);

“FOIA” means the Freedom of Information Act 2000 as amended from time to time and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;

“Force Majeure Event” means, subject to clause 24.4 (*Circumstances beyond either Party’s control*), any event outside the reasonable control of either Party affecting its performance of its obligations under this Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Supplier or the Supplier Staff or any other failure in the Supplier’s or a Subcontractor’s supply chain;

“Force Majeure Notice” means a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;

“**Former Supplier**” means the Awarding Organisation that is operating or operated the T Level technical education qualification under the Original Contract;

"Former Supplier’s TQ" means a technical education qualification forming part of the T Levels Programme which is replaced by the TQ which is the subject of this Contract;

"Former Supplier’s TQ Specification" means the Specification of Content, the Scheme of Assessment and the Approved Provider’s Quality Assurance Process, designed, developed and delivered by a Former Supplier that meets all of the requirements of the Product Description for the TQ Specification; including any TQ Changes required by the Authority notified to the Former Supplier;

“Future Supplier” means any Awarding Organisation appointed, at any point in the future and including any Replacement Supplier, to operate one or more T Level technical education qualifications by or at the direction of the Authority from time to time, and where the Authority is operating a T Level technical education qualification, shall also include the Authority;

“GDPR” means the General Data Protection Regulation (Regulation (EU) 2016/679);

“General Change in Law” means a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which also affects and/or relates to a Comparable Supply;

“Good Industry Practice” means standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;

“Grade Standard Exemplification Materials” means the exemplification materials referred to in, and meeting the requirements of, the relevant part of the Product Description for the Exemplification Materials;

“**Guide Standard Exemplification Materials”** means the exemplification materials referred to in, and meeting the requirements of, the relevant part of the Product Description for the Exemplification Materials and Approved by the Authority;

“IfATE Approval” means approval by the Authority pursuant to section -A2D3 of the Apprenticeships, Skills, Children and Learning Act 2009 for the TQ to be made available to Approved Providers and/or Students based on the TQ meeting the requirements of paragraph 2.1 or 2.3 of Part 1 of the Services Requirements as applicable to the satisfaction of the Authority;

“IfATE Data” means:

(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:
    (i) are supplied to the Supplier by or on behalf of the Authority; or
    (ii) the Supplier is required to generate, process, store or transmit pursuant to this Contract;
(b) any Personal Data for which the Authority is the Controller; or
(c) Student Related Data;

“**Impact Assessment**” means an assessment of the impact of a Variation request completed in good faith, including:

(d) details of the impact of the proposed Variation on the Services (including the supply of the Products) and the Supplier's ability to meet its other obligations under this Contract;

(e) details of the cost of implementing the proposed Variation;

(f) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Charges and/or the Fees (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;

(g) a timetable for the implementation, together with any proposals for the testing of, the Variation; and

(h) such other information as the Authority may reasonably request in (or in response to) the Variation request;

"Implementation and Delivery Plan" means the outline Implementation and Delivery Plan prepared by the Supplier as part of the Supplier's Response for implementation of the Services and supply of the Products (including to meet the Milestones) and which, as at the Effective Date, is set out in Schedule 3 (*Implementatio*n), as such plan is, subject to paragraph 2.5 of Part 1 of the Service Requirements, developed and amended from time to time to fully meet the requirements of the Product Description for the "Implementation and Delivery Plan";

"Inclusive TQ Change" means any TQ Change that is not an Exclusive TQ Change;

"Indemnifier" means a Party from whom an indemnity is sought under this Contract;

"Information Commissioner" means the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;

"Initial Content Date" has the meaning given in clause 8.2 (TQ Changes);

"Initial Development Services" shall have the meaning given in paragraph 2.1 of Part 1 of the Service Requirements;

"Initial Projection" shall have the meaning given in paragraph 2.3 of Schedule 6A (Adaptive Pricing);

"**Initial TQ Deliverables"** means each of:

(i) The TQ Specification;

(j) TQ Specimen Assessment Materials;

(k) the Provider Approval Criteria; and

(l) the Assessment Strategy;

“Insolvency Event” means:

(a) in respect of a company:

(i) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or

(ii) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or

(iii) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or

(iv) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or

(v) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or

(vi) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or

(vii) being a “small company” within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

(b) in respect of an individual or partnership, any event analogous to those listed in limbs (a) (i) to (vii) (inclusive) occurs in relation to that individual or partnership; or

(c) any event analogous to those listed in limbs (a) (i) to (vii) (inclusive) occurs under the law of any other jurisdiction;

“I**ntellectual Property Rights**” or “**IPR**” means:

(i) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other

rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;

(ii) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(iii) all other rights having equivalent or similar effect in any country or jurisdiction;

"**Interim Milestone**" means each of the interim Milestones specified in the Table in Annex 7 to the Service Requirements;

"**Interim Milestone Payment**" means:

(i) in respect of Interim Milestone 1, an amount equal to 30% of the Development Charge;

(ii) in respect of the Interim Milestone 2, an amount equal to 40% of the Development Charge;

"**IPR Claim**" means any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Services and/or supply the Products or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority in the fulfilment of its obligations under this Contract;

"**Issues Log**" means the issues log referred to in, and meeting the requirements of, the Product Description for the Issues Log;

"**Key Dates Schedule**" means a schedule of key dates in relation to the roll-out and operation of the TQ and other technical education qualifications across the T Levels Programme including registration dates and deadlines, assessment dates, and dates for publication of results, which is based on the indicative key dates schedule in Annex 5 to the Service Requirements and is agreed in relation to the T Levels Programme between Awarding Organisations pursuant to Schedule 4 (Co-operation) and Approved by the Authority;

"**Key Materials**" means materials the IPR in which the Authority reasonably requires ownership of for the Portability Purposes. Examples of where the Authority may reasonably require ownership of the IPR include because the Authority or a Future Supplier (or, where relevant, a potential Future Supplier) may need to copy or otherwise reproduce such

materials (in whole or in part), to supply or communicate the same, or to be able control the use (in whole or in part) of such materials by third parties, or to authorise others to do so.

Key Materials shall include:

(i) specifications of content for each TQ including core and all specialist components;

(ii) assessment guidelines (for Providers);

(iii) quality assurance requirements (for Providers);

(iv) specimen assessment materials;

(v) standards exemplification materials;

(vi) supplementary specimen assessment materials;

(vii) employer set project guide exemplar responses;

(viii) employer set project grade exemplar responses;

(ix) updates or redevelopments of specifications of content;

(x) updates and redevelopments of any Key Materials; and

(xi) any materials equivalent to the above to which a Skilled Future Supplier would reasonably require access for the Portability Purposes;

Key Materials shall not include:

1. Support Materials, insofar as they are not part of any of the expressly included items listed above;
2. question banks, insofar as they are not part of any of the expressly included items listed above and are not developed for the TQ; and
3. any systems and platforms used to support the delivery of the TQ, provided that the relevant TQ content or data held in or processed by such systems and/or platforms can be extracted without requiring further processing post-extraction (and the Supplier can demonstrate that they can be so extracted) to enable use of the relevant content and/or data by a Skilled Future Supplier in conjunction with a non-proprietary or generally commercially available system or platform;

"Key Personnel" means the individuals identified as such in the Annex to Schedule 7 (*Staff (including Key Personnel*)) as at the Effective Date or as amended from time to time in accordance with paragraph 1.2 of Schedule 7 (*Staff (including Key Personnel)*);

"Key Roles" means the roles stated in the Annex to Schedule 7 (Staff (including Key Personnel)) as at the Effective Date or as amended from time to time in accordance with paragraph 1.2 of Schedule 7 (Staff (including Key Personnel));

"Key Sub-Contract" means each Sub-Contract with a Key Subcontractor;

"Key Subcontractor" means any Subcontractor:

(a) which is relied upon to deliver any material part of the Services (including to supply any Products); and/or

(b) which, in the opinion of the Authority performs (or would perform if appointed) a critical role in the provision of all or any part of the Services (including the supply of any Products),

and which, as at the Effective Date, are listed in Annex 1 to Schedule 8 (*Supply Chain (including approved Subcontractors)*);

"Know-How" means all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Services and/or the Products;

"KPI" means a key performance indicator applicable to the provision of the Services (including the supply of the Products), as set out in the first column of the Table attached at Annex 1 to Schedule 15 (Monitoring of Performance);

"KPI Improvement Plan" shall have the meaning given in paragraph 2.2 of Schedule 15 (Monitoring of Performance);

"Law" means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;

"Losses" means all losses, liabilities, damages, costs, expenses (including reasonable legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "Loss" shall be interpreted accordingly;

"Management Information" means the management information to be delivered to the Authority by the Supplier, as set out or referred to in Annex 9 to the Service Requirements;

"Mid-term Review" shall have the meaning given in paragraph 1.1.1 of Schedule 6A (Adaptive Pricing);

"Milestone" means an event or task to be performed as part of the provision of the Services (and/or the supply of the Products) by a specific date as described in the first column of the Table in Annex 7 to the Service Requirements;

"Moderation" means the Supplier assessment process designed to ensure that, where Approved Provider marking is undertaken in accordance with the Approved Assessment Strategy, such marking is scrutinised by a Moderator to ensure that it is in line with expected standards and Students' marks are adjusted where necessary; and "Moderate" will be construed accordingly;

"Moderator" means a moderator, external to the Approved Provider, employed or engaged by the Supplier to moderate marking undertaken by assessors employed or engaged by the Approved Provider of Students' performance in respect of the TQ Live Assessment Materials;

"Month" means a calendar month and "Monthly" shall be interpreted accordingly;

"National Insurance" means contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;

"Notified Sub-contractor" means a Sub-contractor to whom Transferring Former Supplier Employees will transfer on a Relevant Transfer Date;

"Occupation" means a set of jobs where the main tasks and duties are characterised by a high degree of similarity, where a "job" is a role connected to a specific employment contract in a workplace;

"Occupational Map" means, for each Route, a map which groups Occupations according to where there is a requirement for shared technical knowledge, skills, and behaviours, and identifies the Occupations for which Standards exist;

"Occupational Standard" means the description of the Occupation and the outcomes (knowledge, skills and behaviours) which a Student will be expected to attain to successfully achieve competence in that Occupation, as approved and published by the Authority;

"Occupational Specialist Component" means each occupational specialist component of the TQ as referred to in the Former Supplier's TQ Specification and/or if relevant, the Outline Content;

"Ofqual" means the Office of Qualifications and Examinations Regulation, a statutory body created under the Apprenticeships, Skills, Children and Learning Act 2009, as amended by the Education Act 2011, to regulate qualifications, examinations and assessments in England;

"Ofqual Recognition" means recognition of the Supplier by Ofqual in respect of the TQ under section 132 of the Apprenticeships, Skills, Children and Learning Act 2009;

"Ongoing Development Services" shall have the meaning given in paragraph 2.3 of Part 1 of the Service Requirements;

"Operate" in relation to a qualification means to provide the Services or a material part of the Services, or services replacing the Services or a material part of the Services, or of an equivalent character to the Services or a material part of the Services in relation to any other qualification (whether a TQ or not); and "Operation" and other cognate terms shall have a corresponding meaning;

"Operational Delivery Report" means the report referred to in the third row of the first column in the Table in Annex 9 to the Service Requirements and containing the information set out in the third row of the second column of that Table;

"Ordinary Exit" means any termination of this Contract (other than an Early Exit) that occurs as a result of the expiry of the Contract on the Expiry Date (as extended by any Extension Period);

"Original Contract" means the contract entered into between the Authority and the Former Supplier for the provision of Services (including the supply of any Products) for the TQ prior to the Effective Date of this Contract and remains in place until the end of the Entry Transition Period;

"Outline Content" means the outline content developed for the TQ by the Authority;

"Parliament" takes its natural meaning as interpreted by Law;

"Party" means the Authority or the Supplier and "Parties" means both of them where the context permits;

"Pathway" means a sub-set of a Route, which groups common sets of Occupations into a number of occupational clusters together;

"Performance Monitoring Methodology" means the required evidence and measurement methodology that is to be applied by the Supplier to assess its performance of the relevant part of the Services (including the supply of any Products) to which the KPI in question relates, as such evidence and measurement methodology are set out in the fifth and sixth columns (respectively) of the Table attached at Annex 1 to Schedule 15 (Monitoring of Performance);

"Performance Monitoring Period" means the period set out against the relevant KPI in the fourth column of the Table attached at Annex 1 to Schedule 15 (Monitoring of Performance);

"Performance Review Meeting" shall have the meaning given in paragraph 3.2 of Schedule 15 (Monitoring of Performance);

"Personal Data" means "personal data" (as defined in the GDPR) that are processed under this Contract;

"**Portability Purposes"** means in order:

a) to secure a smooth transition to a Skilled Future Supplier;
b) to enable the Authority to procure a Skilled Future Supplier (including inviting competition and/or tenders), and for a potential Skilled Future Supplier to compete openly and effectively in any future competition or tender for, delivery and/or Operation of the TQ currently delivered by the Supplier and/or a Replacement TQ;
c) to enable a Skilled Future Supplier to deliver and/or Operate the TQ and/or a Replacement TQ; to enable the Authority and/or any Skilled Future Supplier to carry out or have carried out any Continuing Activities; and/or
d) to enable a Skilled Future Supplier to supply, to Providers, the TQ and/or Replacement TQ and sufficient information and materials (including Support Materials) for Providers to deliver the TQ in a Transparent manner;

"Post-Results Services" means the Services described in and/or provided pursuant to paragraph 9 of Part 1 of the Service Requirements, including the Additional Services;

"**Pre-Delivery Phase**" means the period between the Approval of the TQ and the first teaching of the TQ by Providers, being the period during which Supplier and Providers prepare for delivery;

"Prescribed Person" means a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 5 October 2019, available online at:
https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies;

"Processor" has the same meaning as in the GDPR and "Processing"; and "Processed" shall be interpreted accordingly;

"Product" means each product listed in the first column of the Table in Part 3 of the Service Requirements;

"Product Description" means the description of the Authority's minimum requirement for the relevant Product set out in the second column of the Table in Part 3 of the Service Requirements, together with such further information, data and/or content as should reasonably be expected by the Supplier having regard to the Authority's requirements under this Contract and the Supplier's obligations under clause 3.1 (How the Services must be supplied);

"Prohibited Acts" means:

(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority or any other public body a financial or other advantage to:
  (i) induce that person to perform improperly a relevant function or activity; or
  (ii) reward that person for improper performance of a relevant function or activity;

(b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Contract; or

(c) committing any offence:
  (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or
  (ii) under legislation or common law concerning fraudulent acts; or
  (iii) defrauding, attempting to defraud or conspiring to defraud the Authority or other public body; or

(d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;

"Provider" means an organisation that has a grant agreement and/or a contract in place with the ESFA to provide qualifications to Students or that provides such services on a privately funded basis;

"Provider Approval" means approval of the Eligible Provider in accordance with clause 7.1 (Interaction with Providers);

"Provider Approval Criteria" means the approval criteria referred to in, and meeting the requirements of, the Product Description for the Provider Approval Criteria;

"Provider Contract" means a contract between an Approved Provider and the Supplier in respect of the TQ meeting the requirements set out in Schedule 17 (Provider Contract requirements);

"Provider Services" means the Services, other than the Initial Development Services and the Ongoing Development Services;

"Rate Card" means the Supplier's rate card as set out in Schedule 6 (Pricing Schedule);

"Reasonable Adjustments" shall have the meaning given in SR 2.4 of Service Requirement 2 (as defined in the Service Requirements);

"Recipient Party" means the Party which receives or obtains directly or indirectly Confidential Information;

"Reduced Entry Fee" shall have the meaning given in paragraph 2.4 of Schedule 6A (Adaptive Pricing);

"Reduced Extension Entry Fee" shall have the meaning given in paragraph 3.3 of Schedule 6A (Adaptive Pricing);

"Regulated" means the regulation by Ofqual of a qualification which has been Accredited and "Regulation" shall be authorised accordingly;

"Regulations" means the Concession Contracts Regulations 2016;

"Relevant Competence" means being a reasonably skilled and competent Awarding Organisation with access to appropriate tools, systems and platforms to operate technical qualifications;

"Relevant Employees" means those employees whose contracts of employment transfer with effect from the Relevant Transfer Date to the Authority or a Replacement Supplier by virtue of the application of TUPE;

"Relevant Requirements" means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;

"Relevant Transfer" means a transfer of employment to which TUPE applies;

"Relevant Transfer Date" means in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place;

"Reminder Notice" means a written notice sent in accordance with clause 4.8 (Pricing and payments) given by the Supplier to the Authority providing notification that payment has not been received on time, which must be addressed to the Authority Authorised Representative, must set out the sum due, must reference this Contract and clause 4 (Pricing and payments) and attach a copy of the relevant valid invoice;

"Replacement Subcontractor" means a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);

"Replacement Services" means any services (including the supply of products) which are the same as or substantially similar to any of the Services and which the Authority receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Contract, whether those services are provided by the Authority internally and/or by any third party;

"Replacement Supplier" means any third party provider of Replacement Services appointed by or at the direction of the Authority from time to time, or where the Authority is providing Replacement Services on its own account, shall also include the Authority;

“Replacement TQ” means a technical education qualification forming part of the T Levels Programme to replace either: (i) the TQ which is the subject of this Contract; or (ii) the equivalent technical qualification which is the subject of a contract with a Future Supplier;

“Request for Information” means a request for information or an apparent request for information relating to this Contract or an apparent request for such information under the FOIA or the EIRs;

“Required Insurances” means the insurances that must be held by the Supplier as required by the Authority meeting the requirements set out in Schedule 19 (Required Insurances);

“Resource Plan” means the Resource Plan prepared by the Supplier as part of the Supplier’s Response in relation to the Supplier Staff that shall be utilised (and the manner in which such Supplier Staff shall be utilised) by the Supplier in the performance of the Services and which, as at the Effective Date, is set out in Schedule 3 (Implementation), as such plan is, subject to paragraph 2.5 of Part 1 of the Service Requirements, developed and amended from time to time to fully meet the requirements of the Product Description for the “Resource Plan”;

“Re-Submission” shall have the meaning given in clause 5.11.2(i) (Developing the TQ and achieving IfATE Approval);

“Risk Register” means the risk register referred to in, and meeting the requirements of, the Product Description for the Risk Register;

“Route” means the broadest category of Occupations in an Occupational Map, typically covering an industrial area;

“Route Panel” means the Authority’s panel responsible for managing the development of the TQ Specification, details of which can be found at:
https://www.gov.uk/government/publications/t-level-panels-membership;

“Scheme of Assessment” means the scheme of assessment referred to in, and meeting the requirements of, the relevant part of the Product Description for the TQ Specification;

“Security Policy” means the Authority's security policy, in force as at the Effective Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;

“Serious Fraud Office” means the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;

“Services” means the services as described in the Service Requirements (including the Additional Services);

“Service Failure” shall have the meaning given in paragraph 2.2 of Schedule 15 (Monitoring of Performance);

“Service Requirements” means the Authority’s requirements for the Services (including the supply of the Products) as set out in Schedule 2 (Service Requirements);

“Service Transfer” means any transfer of the Services (or any part of the Services), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;

“Service Transfer Date” means the date of a Service Transfer;

“Skilled Future Supplier” means a Future Supplier with Relevant Competence;

“Social Value” means the additional social benefits that can be achieved in the delivery of the Contract, set out in the Supplier’s Response and/or Supplier’s Tender;

“Special Consideration” shall have the meaning given in SR 2.5 of Service Requirement 2 (as defined in the Service Requirements);

“Specific Change in Law” means a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Services and/or the Products and/or the performance of this Contract is not reasonably foreseeable at the Effective Date. Any change in any Condition of Recognition shall not be a Specific Change in Law;

“Specification of Content” means the specification of the content referred to in, and meeting the requirements of, the relevant part of the Product Description for the TQ Specification;

“Staffing Information” means in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Authority may reasonably request (subject to all applicable provisions of the Data Protection Legislation), but including in an anonymised format:

(e) their ages, dates of commencement of employment or engagement, gender and place of work;
(f) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;
(g) the identity of the employer or relevant contracting Party;
(h) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;
(i) their wages, salaries, bonuses and profit sharing arrangements as applicable;
(j) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;
(k) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);
(l) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;
(m) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and
(n) any other Employee Liability Information" as such term is defined in regulation 11 of TUPE;

"Stakeholders" means the Authority, the Department, ESFA, Ofqual, Providers, Employers and members of the Route Panels;

"Standards" means the Occupational Standards, consisting of a description of the Occupation and the outcomes (knowledge, skills and behaviours) which a Student will be expected to attain to successfully achieve competence in that Occupation, as approved and published by the Authority;

"Storage Media" means the part of any device that is capable of storing and retrieving data;

"Student" means an individual undertaking (or who wishes to undertake) a formal programme of study with an Approved Provider for the T Level of which the TQ forms part;

"Student Information" means information or data relating to an individual Student whether or not the Student can be identified from that information or data;

“Student Related Data” means any information or data relating to Students (including any Student Information) and/or any Provider which is generated and/or acquired by and/or otherwise comes into the possession of the Supplier and/or any Supplier Staff as a result of the performance of the Supplier’s obligations under this Contract;

“Sub-Contract” means any contract or agreement (or proposed contract or agreement), pursuant to which a third party:

(o) provides the Services and/or supplies any Products (or any part of them) and/or performs the whole or any part of this Contract;

(p) provides facilities or services necessary for the provision of the Services and/or the supply of any Products (or any part of them) and/or the performs the whole or any part of this Contract; and/or

(q) is responsible for the management, direction or control of the provision of the Services and/or supply of any Products (or any part of them) and/or the performance of the whole or any part of this Contract;

“Subcontractor” means any person other than the Supplier (and/or an Assessor who is self-employed or who provides services to the Supplier through that Assessor’s own personal service company), who is a party to a Sub-Contract and the servants or agents of that person;

“Submission” means, in respect of the relevant Milestone, the Products set out against that Milestone in the third column of the Table in Annex 7 to the Service Requirements;

“Submission Date” means, in respect of the relevant Milestone, the date set out against that Milestone in the second column of the Table in Annex 7 to the Service Requirements;

“Submission Issues Log” means the issues log referred to in, and meeting the requirements of, the Product Description for the Submission Issues Log;

“Subsequent Transfer” has the meaning given in paragraph 8.1 of Schedule 12 (Exit Management);

"Supplementary Specimen Assessment Materials" means a full suite of sample questions and tasks for the Core Component and Occupational Specialist Component(s) (in addition to the TQ Specimen Assessment Materials), as referred to in Service Requirement 5.1;

“Supplier Authorised Representative” means the person referred to in Schedule 20 as such or the representative appointed by the Supplier from time to time in relation to this Contract as notified in writing (which may, in the case of this specific notification, be by email only) to the Authority;

“Supplier Personnel” means all employees of the Supplier (and any subcontractor) who are wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services including the development of the Products;

“Supplier Staff” means all directors, officers, employees, agents, consultants and contractors of the Supplier (including any Assessor who is self-employed or who provides services to the Supplier through that Assessor’s own personal service company), any Subcontractor engaged in the performance of the Supplier's obligations under this Contract and any company or organisation noted in the Supplier’s Tender as forming part of the consortium which submitted the Supplier’s Tender (“Consortium Member”) and all directors, officers, employees, agents, consultants and contractors of any such Subcontractor and/or any such Consortium Member engaged in the performance of the Supplier's obligations under this Contract;

“Supplier's Final Supplier Personnel List” means a list provided by the Supplier of all Supplier Personnel whose will transfer under TUPE on the Service Transfer Date;

“Supplier’s Provisional Supplier Personnel List” means a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;

“Supplier’s Response” means that part of the Supplier’s Tender (including any method statements) which is at Schedule 5 (Supplier’s Response);

“Supplier’s Tender” means the Supplier’s selection questionnaire and tender responses submitted in response to the Authority’s advertisement in the Find a Tender Service (as referred to in the Recitals to this Contract) for a provider of the Services and supplier of the Products, as clarified in writing by the Supplier to the Authority prior to the date of this Contract in response to any request for clarification issued by the Authority;

“Supplier Termination Event” means:

(a) the Supplier (i) commits a material Default which is irremediable; or (ii) commits a material Default which is capable of remedy, but which has not been remedied by the Supplier within 30 days of being notified in writing to do so by the Authority;

(b) a Conflict of Interest arises in connection with the delivery of the Services (and/or the supply of the Products) to which no mitigation acceptable to the Authority can be promptly identified;

(c) where a right of termination is expressly reserved in this Contract;

(d) the Supplier is in material Default in respect of any data handling and/or security requirements set out in clauses 13, 18, 19 or Schedule 9 (*Data Handling and Security Management*) (where applicable);

(e) an Insolvency Event occurring in respect of the Supplier.

(f) a change of Control of the Supplier.

(i) the Authority has given its prior written consent (not to be unreasonably withheld or conditioned) to the particular change of Control, which subsequently takes place as proposed; or

(ii) the Authority has not served its notice of objection within 6 months of the later of the date on which the change of Control took place or the date on which the Authority was given notice of the change of Control;

(g) a material failure by the Supplier to comply with legal obligations in the fields of environmental, social or labour law;

(h) the departure from the Supplier of any of its senior officers or Key Personnel where the Authority has reasonable grounds to believe that such departure will impact or could potentially impact the delivery of the Services and/or the supply of any Products unless the Authority has not served its notice of objection within 6 months of the date on which the Authority was informed by the Supplier of such departure;

(i) the Supplier assigns, transfers or otherwise disposes of its rights, obligations and/or liabilities or seeks to assign, transfer or otherwise dispose of its rights, obligations and/or liabilities under the whole or any part of this Contract to a third party in breach of the terms of this Contract (including in breach of the requirements of paragraph 1 of Schedule 8 (*Supply Chain (including approved Subcontractors)*);

(j) the Supplier is in Default under clause 31.1 (*Preventing Fraud, Bribery and Corruption*);

(k) the Supplier provided incorrect or misleading information as part of the Supplier's Tender;

(l) the Supplier or any Subcontractor or Affiliate through its act or omission brings the Authority, the Department and/or the ESFA and/or the T Levels Programme into

disrepute and/or diminishes the trust the public places in the Authority, the Department and/or the ESFA;

(m) Not used.

(n) an occurrence of any of the circumstances in regulations 44(1) (a) to (c) of the Regulations;

(o) this Contract has been substantially modified in breach of regulation 43(10) of the Regulations;

(p) the Authority discovers that the Supplier was in one of the situations in regulations 38(8) to 38(10) of the Regulations at the time this Contract was awarded;

(q) the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union ("**TFEU**") to declare that this Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations;

(r) a Critical Service Failure occurs; or

(s) the Supplier fails to comply with clause 35.2 (*Tax*) or fails to provide details of steps being taken and mitigating factors pursuant to clause 35.2 (*Tax*) which in the reasonable opinion of the Authority are acceptable;

"Support Materials" means teaching support materials intended for a Provider or Student audience, such as textbooks, and any other materials which the Authority agrees in writing to be Support Materials;

"Target Service Level" means the target performance level set out against the relevant KPI in the third column of the Table attached at Annex 1 to Schedule 15 (Monitoring of Performance);

"Technical Qualifications Explanatory Note" means an explanation of TQs, their purpose and how they are delivered;

"Term" means the period commencing on the Effective Date and ending on the End Date;

"Termination Notice" means a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Contract on a specified date and setting out the grounds for termination;

"Third Party" means any supplier of services fundamentally the same as the Services (either in whole or in part) immediately before the Effective Date;

"Third Party IPR" means Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Services and/or supplying the Products;

"Transferring Former Supplier Employees" means those employees of the Former Supplier to whom TUPE will apply on a Relevant Transfer Date;

"TQ" means the technical education qualification element of the T Level in respect of the Pathway that is (amongst other things) designed, developed and delivered under this Contract;

"TQ Assignment and Licence" means the assignment and licence in respect of certain Intellectual Property Rights in relation to the TQ in the form set out in Schedule 14 (Form of Assignment and Licence);

"TQ Change" means any change or variation to the content of the TQ;

"TQ Content Updating Schedule" means the schedule of dates set out in Annex 6 to the Service Requirements (or such other dates as may be agreed by the Authority from time to time) applicable to the relevant Inclusive TQ Change or Exclusive TQ Change (as the case may be);

"TQ Core Component" means the core component of the TQ referred to in the Former Supplier's TQ Specification and/or if relevant, the Outline Content;

"TQ Deliverables" means:

(a) in the period prior to the Supplier making available the Grade Standard Exemplification Materials referred to in paragraph 6.2.2 of Part 1 of the Service Requirements, the Approved Initial TQ Deliverables and the Approved Guide Standard Exemplification Materials; and

(b) in the period following the Supplier making available the Grade Standard Exemplification Materials referred to in paragraph 6.2.2 of Part 1 of the Service Requirements:

(i) the Approved Initial TQ Deliverables; and

(ii) the Grade Standard Exemplification Materials,

in each case, as amended in accordance with this Contract;

"TQ Development Meeting" shall have the meaning given in clause 5.4 (Developing the TQ and achieving IfATE Approval);

"TQ Live Assessment Materials" shall have the meaning given in Schedule 2 (Service Requirements);

"TQ Specification" means the Specification of Content, the Scheme of Assessment and the Approved Provider's Quality Assurance Process;

"TQ Specimen Assessment Materials" means the specimen assessment materials referred to in, and meeting the requirements of, the Product Description for the TQ Specimen Assessment Materials;

"T Level" means the technical study programme known as a **"T Level";**

"T Level Awarding Organisations" shall have the meaning given in paragraph 1.1 of Schedule 4 (Co-operation);

"T Level Branding Guidelines" means the Authority's written guidelines prescribing the permitted form and manner in which the trade marks (the "Mark" as defined within the T Level Trade Mark Licence) may be used and setting out how the Supplier branding may be used in relation to materials used in the operation of the TQ or to promote the TQ, a copy of which is set out in the document entitled T Level Branding Guidelines, including any amendments or additions notified by the Authority to the Supplier from time to time, provided that the Authority shall where possible provide reasonable notice in writing to the Supplier of any proposed amendments or additions to such guidelines;

"T Level Panel" means the group of Employers, professionals and practitioners appointed to advise on the content of the T Level of which the TQ forms part;

"T Level Trade Mark Licence" means the trade mark licence granted pursuant to Schedule 16 (Logos and Trademarks – T Level Trade Mark Licence);

"T Levels Programme" means the programme of technical education in England managed by the Authority and known as "T Levels";

"Transferable Contracts" means Sub-Contracts, or other agreements which are necessary to enable the Authority or any Replacement Supplier to provide the Services

and/or develop, maintain or supply the Products or the Replacement Services, including all relevant Documentation;

"Transferring Supplier Employee" means those employees whose contract of employment will be transferred to the Authority or a Replacement Supplier pursuant to TUPE on expiry or termination of this Contract;

"Transition Period" means the period from a Replacement Supplier or Future Supplier commencing any aspects of development or delivery of the TQ to the End Date, eg from the point when the Replacement Supplier or Future Supplier has been awarded a contract for provision of the TQ, but while this Contract remains in place for existing Students;

"Transparency Information" has the meaning given to it in clause 20 (When information can be shared);

"Transparency Reports" means: (i) the Management Information relating to the Services and performance of this Contract which the Supplier is required to provide to the Authority in accordance with the reporting requirements set out in the Service Requirements; and (ii) the output of any survey commissioned by the Authority in connection with the performance of the Supplier under this Contract;

"Transparent" means that Students and Employers will regard the TQ delivered by a Future Supplier as materially the same as the TQ delivered and operated by the (existing) Supplier;

"TUPE" means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (2006/246) and/or any other regulations or other legislation enacted for the purpose of implementing or transposing the Acquired Rights Directive (77/187/EEC, as amended by Directive 98/50 EC and consolidated in 2001/23/EC) into English law;

"TUPE Information" has the meaning given in paragraph 8.5 of Schedule 12 (Exit Management);

"Updated Projection" shall have the meaning given in paragraph 2.1 of Schedule 6A (Adaptive Pricing);

"Variation" means any variation or change to this Contract which is not an Inclusive TQ Change;

“Variation Form” means the form set out in Schedule 11 (Change Management);

“VAT” means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and

“Working Day” means any day other than a Saturday or Sunday or public holiday in England and Wales.

Schedule 2

Service Requirements

The content for this Schedule is contained in a separate file at:

S2_GEN2W1_DSS_Service_Requirements

S2_A3_GEN2W1_DSS_TQ_Spec

Schedule 2

Service Requirements

S2_GEN2W1_DSS_Service_Requirements

Schedule 2

Service Requirements

Definitions

In this Service Requirements, the following terms shall have the following meanings:

"**Appeal**" shall have the meaning given in SR 8.2 in Service Requirement 8;

"**Approved Assessment Strategy**" means the Assessment Strategy approved by the Authority in accordance with clause 5.13 (*Developing the TQ and achieving IfATE Approval*) or clause 8 (*TQ Changes*) (as the case may be), subject to paragraph 2.6 of Part 1 of the Service Requirements, as amended from time to time in accordance with this Contract;

"**Approved Guide Standard Exemplification Materials**" means the Guide Standard Exemplification Materials approved by the Authority in accordance with clause 5.13 (*Developing the TQ and achieving IfATE Approval*) subject to paragraph 2.6 of Part 1 of the Service Requirements, as amended from time to time in accordance with this Contract;

"**Component**" means the TQ Core Component or any Occupational Specialist Component (as the case may be) and "**Components**" shall mean both or all of them (as the context may require);

"**Employer Set Project"** means a project set collaboratively between the Supplier and Employers, as more particularly referred to in Service Requirement 2;

"**External Examination"** means each assessment by examination which is:

(a) set by the Supplier;

(b) designed to be taken simultaneously by all Students taking the relevant assessment at a time (subject to compliance with the requirements of the Key Dates Schedule for the relevant Academic Year) determined by the Supplier;

(c) taken under conditions specified by the Supplier (including conditions relating to the supervision of Students taking the relevant assessment and the duration of the assessment); and

(d) marked by the Supplier.

"**First Teach Cohort**" means the first group of Students to be assessed on the TQ;

"**Guided Learning**" means the activity of a Student being taught or instructed by, or otherwise participating in education or training under the immediate guidance or supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training. For these purposes the activity of 'participating in education or training' shall be treated as including the activity of being assessed if the assessment takes place under the immediate guidance or supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training;

"**Occupational Entry Competence**" means that level of competence that:

(a) signifies that a Student is well-placed to develop full occupational competence, with further support and development, once in employment;

(b) is as close to full occupational competence as can be reasonably expected of a Student studying the TQ in a classroom-based setting (e.g. in the classroom, workshops simulated working and (where appropriate) supervised working environments); and

(c) signifies that a Student has achieved the level for a pass in relation to the relevant Occupational Specialist Component;

"**Qualification Purpose**" means the purpose of the TQ set out in Annex 1 of this Service Requirements;

"**Service Definition Table**" means the Table set out in Part 2 of this Service Requirements;

"**Service Requirement 1**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 1: Designing, developing and managing TQ Content" in the Service Definition Table;

"**Service Requirement 2**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 2: Assessment Design and Delivery" in the Service Definition Table;

"**Service Requirement 3**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 3: Grading and Awarding" in the Service Definition Table;

"**Service Requirement 4**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 4: Provider Approval" in the Service Definition Table;

"**Service Requirement 5**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 5: Provider Support" in the Service Definition Table;

"**Service Requirement 6**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 6: Student registration and Student entry" in the Service Definition Table;

"**Service Requirement 7**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 7: TQ Results" in the Service Definition Table;

"**Service Requirement 8**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 8: TQ Post-Results Services" in the Service Definition Table;

"**Service Requirement 9**" means that part of the Services (including the requirements for and the outcomes to be achieved by the Supplier as a result of the performance of that part of the Services) set out or referred to under the heading of "Service Requirement 9: Reporting" in the Service Definition Table;

"**TQ Critical Path Diagram**" means the diagram setting out the critical path for the design, development and delivery of the TQ attached at Annex 4 to the Service Requirements;

“**TQ Live Assessment Materials**” means the live assessment materials referred to in, and meeting the requirements of, the Product Description for the TQ Live Assessment Materials.

Part 1 – Overview of the Service Requirements

1 Introduction

1.1 This Part 1 of this Service Requirements sets out:

1.1.1 at paragraph 2, that part of the Services relating to the design, development and delivery of the Initial TQ Deliverables and Guide Standard Exemplification Materials and the review and update of such Initial TQ Deliverables and/or the TQ Deliverables (as the case may be), including the Initial Development Services and the Ongoing Development Services;

1.1.2 at paragraph 3, that part of the Services relating to the Provider Approval and monitoring services (as detailed in that paragraph 3);

1.1.3 at paragraph 4, that part of the Services relating to the support to be provided to Eligible Providers and Approved Providers (as detailed in that paragraph 4);

1.1.4 at paragraph 5, that part of the Services relating to Student registration and Student assessment entry (including Additional Services) (as detailed in that paragraph 5);

1.1.5 at paragraph 6, that part of the Services relating to the design and delivery of the TQ Live Assessment Materials (as detailed in that paragraph 6);

1.1.6 at paragraph 7, that part of the Services relating to grading and awarding in respect of each Student's performance in respect of the TQ Live Assessment Materials (as detailed in that paragraph 7);

1.1.7 at paragraph 8, that part of the Services relating to the provision of results (as detailed in that paragraph 8);

1.1.8 at paragraph 9, that part of the Services relating to the provision of Post-Results Services (including Additional Services) (as detailed in that paragraph 9);

1.1.9 at paragraph 10, that part of the Services relating to the reporting of Management Information (as detailed in that paragraph 10); and

1.1.10 at paragraph 11, such other services as may be necessary to support and/or are associated with the provision of the Services (as detailed in that paragraph 11).

1.2 Paragraphs 2 (*Initial TQ Deliverables and development services*) to 9 (*TQ Post-Results Services*) shall be read in conjunction with the TQ Critical Path Diagram.

1.3 The Supplier shall design, develop, obtain IfATE Approval for, and deliver to Approved Providers in England, the technical qualification element of the T Level for the relevant Pathway under this Contract, including, without prejudice to its obligations in clause 3.1.8 (*How the Services must be supplied*), performing all of the Services set out in this Service Requirements.

1.4 Unless otherwise stated in this Service Requirements, the Supplier shall organise and deliver the Services:

1.4.1 to ensure that the activities contemplated by the Key Dates Schedule for the relevant Academic Year and/or the TQ Content Updating Schedule (and which rely on the performance of the whole or any part of the Services) can be carried out and completed in accordance with such Key Dates Schedule and/or the TQ Content Updating Schedule (as the case may be);

1.4.2 in accordance with the Implementation and Delivery Plan;

1.4.3 in accordance with the Resource Plan;

1.4.4 in accordance with the Approved Assessment Strategy; and

1.4.5 (at all times) taking into account the aims of the Qualification Purpose.

1.5 The Supplier shall, subject to paragraphs 2.5 and 2.6 (*Initial TQ Deliverables and development services*) and paragraph 6.3 (*TQ live assessment design and delivery*) and without prejudice to paragraph 2.1 to 2.4 (*Initial TQ Deliverables and development services*) (inclusive), provide a copy of any Products that are developed, amended, updated and/or supplemented from time to time by the Supplier in accordance with this Contract to the Authority as soon as reasonably practicable following such development, amendment, update and/or supplement.

1.6 If there is any conflict and/or inconsistency between the provisions of this Service Requirements and the Conditions of Recognition, the Conditions of Recognition shall prevail.

1.7 Without prejudice to paragraph 1.4.1, the Supplier shall organise and deliver the Services to ensure that all applicable parts of the Services are provided at such times and in such manner as shall be necessary to facilitate the delivery of the number of assessment series for the TQ as shall be contemplated by the Key Dates Schedule for the relevant Academic Year, subject always to the provisions of paragraphs 1.8 to 1.10 (inclusive).

1.8 The Supplier shall ensure that there shall be at least one, but not more than two, assessment series in each Academic Year in respect of each of the assessments for:

1.8.1 the TQ Core Component (comprising the External Examination and the Employer Set Project); and

1.8.2 the Occupational Specialist Components.

1.9 The Supplier acknowledges that the assessments in each Academic Year for the TQ Core Component and the Occupational Specialist Components referred to in paragraph 1.8 may be, but are not required to be, held in the same assessment series and so therefore can be for example:

1.9.1 provided in a single assessment series (encompassing both such assessments for the TQ Core Component and the Occupational Specialist Components); or

1.9.2 provided in two assessment series (for each of such assessments for the TQ Core Component and the Occupational Specialist Components) being a total of four assessment series.

1.10 The Supplier shall ensure that:

1.10.1 each Student takes all of the assessments for the TQ Core Component referred to in paragraph 1.8.1;

1.10.2 each Student takes all of the assessments for each individual Occupational Specialist Component referred to in paragraph 1.8.2 in the same assessment series;

1.10.3 a Student may, subject to paragraphs 1.10.1 and 1.10.2, take the assessments for the TQ Core Component and the Occupational Specialist Components referred to in paragraph 1.8 in different assessment series (including assessment series in different Academic Years); and

1.10.4 its approach to the scheduling of the assessments shall be set out in its Assessment Strategy.

2 Initial TQ Deliverables and development services

Initial Development Services

2.1 Without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*) and clause 5 (*Developing the TQ and achieving IfATE Approval*), the Supplier shall design, develop and deliver the Initial TQ Deliverables in accordance with (and meeting all of the requirements of):

2.1.1 the Product Description for each item forming part of the Initial TQ Deliverables;

2.1.2 the Former Supplier's TQ Specification and/or ,if relevant, the Outline Content;

2.1.3 the requirements set out in the third column of Service Requirement 1, Service Requirement 2, Service Requirement 3 and Service Requirement 4;

2.1.4 the Implementation and Delivery Plan (including the Supplier's obligation to work with and consult (and take into account the outcome of such working with and consultation of) a representative sample of Providers and Employers (as required by that Implementation and Delivery Plan);

2.1.5 the Resource Plan;

2.1.6 the Assessment Strategy; and

2.1.7 Annex 7 (*Initial Development Milestones*) to this Service Requirements,

and, in each case, to ensure the delivery of a high quality technical education qualification element of the T Level for the relevant Pathway and that the outcomes referred to in the first column of Service Requirement 1, Service Requirement 2, Service Requirement 3 and Service Requirement 4 are achieved (the "**Initial Development Services**").

2.2 The Supplier shall procure that, without prejudice to its obligations in clause 5.13.2 (*Developing the TQ and achieving IfATE Approval*), the Initial TQ Deliverables

(meeting all of the requirements of paragraph 2.1) shall be delivered to the Authority on or prior to the Final Approval Milestone Date.

Ongoing Development Services

2.3 The Supplier shall procure that (without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*) and clause 5.3 (*Developing the TQ and achieving IfATE Approval*) and notwithstanding the achievement of IfATE Approval in respect of the Initial TQ Deliverables) throughout the Term the TQ Deliverables meet (and continue to meet) all of the requirements of:

2.3.1 the Product Description for each item forming part of the TQ Deliverables;

2.3.2 the Former Supplier's TQ Specification and, if relevant, the Outline Content;

2.3.3 the requirements set out in the third column of Service Requirement 1, Service Requirement 2, Service Requirement 3 and Service Requirement 4;

2.3.4 the Implementation and Delivery Plan (including the Supplier's obligation to work with and consult (and take into account the outcome of such working with and consultation of) a representative sample of Providers and Employers (as required by that Implementation and Delivery Plan));

2.3.5 the Resource Plan;

2.3.6 the Approved Assessment Strategy; and

2.3.7 clause 8 (*TQ Changes*) and Annex 6 (*TQ Content Updating Schedule*) to this Service Requirements,

and in each case, to ensure the continued delivery of a high quality technical education qualification element for the T Level for the relevant Pathway and that the outcomes referred to in the first column of Service Requirement 1, Service Requirement 2, Service Requirement 3 and Service Requirement 4 are achieved (the "**Ongoing Development Services**").

2.4 The Supplier shall procure that the TQ Deliverables (as amended, supplemented or replaced in accordance with clause 8 (*TQ Changes*) and Annex 6 (*TQ Content Updating Schedule*) to this Service Requirements) shall be delivered to the Authority

on or prior to the applicable date specified on the Key Dates Schedule for the relevant Academic Year or TQ Content Updating Schedule (as applicable).

Updating the Implementation and Delivery Plan and the Resource Plan

2.5 Subject to the provisions of paragraph 3 *(Key Personnel)* of Schedule 7 *(Staff including Key Personnel)*, the Parties acknowledge and agree that the Implementation and Delivery Plan and the Resource Plan are intended to be live documents that may need to flex from time to time to ensure the continued successful delivery of the Services to the standards required by this Contract and the Supplier shall, throughout the Term, review, amend and update (as necessary) each of the Implementation and Delivery Plan and the Resource Plan to ensure that such Implementation and Delivery Plan and Resource Plan takes into account (and (where applicable) mitigates the effects of) all relevant factors that have impacted or may impact upon the successful delivery of the Services to the standards required by this Contract, provided always that where any such review, amendment and/or update would (or is reasonably likely to) operate to reduce and/or otherwise diminish the Authority's rights and/or remedies and/or the Supplier's liabilities contemplated by this Contract (including where, but for such review, amendment and/or update, the Supplier would (or would be reasonably likely to) be in Default under this Contract), the Supplier shall:

2.5.1 submit such proposed reviewed, amended and/or updated Implementation and Delivery Plan and/or Resource Plan (as the case may be) to the Authority for Approval; and

2.5.2 where the Supplier does not obtain such Approval, the Implementation and Delivery Plan and/or Resource Plan (as the case may be) shall be deemed not to have been so reviewed, amended and/or updated to the extent that such review, amendment and/or update would (or would be reasonably likely to) operate to so reduce the Authority's rights and/or remedies and/or the Supplier's liabilities under this Contract.

Updating the Approved Initial TQ Deliverables and TQ Deliverables

2.6 The Supplier shall, notwithstanding the achievement of IfATE Approval in relation to the Initial TQ Deliverables and subject to the provisions of clauses 8.4 and 8.5 (*TQ Changes*) and Annex 6 (*TQ Content Updating Schedule*) to this Service Requirements (which shall apply in respect of the annual review referred to in such clauses 8.4 and 8.5 (*TQ Changes*)), be required to keep under review, and entitled to amend and update, the Approved Initial TQ Deliverables and the TQ Deliverables throughout the

Term to ensure that the Supplier continues to meet its obligations under paragraph 2.3, provided always that the Supplier shall:

2.6.1 notify the Authority (as part of the Operational Delivery Report) of any proposed amendments and/or updates to such Approved Initial TQ Deliverables and/or TQ Deliverables; and

2.6.2 comply with the applicable requirements of clauses 8.10 and 8.11 (*TQ Changes*) prior to making available any such amended and/or updated Approved Initial TQ Deliverables and/or TQ Deliverables to Approved Providers and provided further that the words "*by the relevant date prescribed by the TQ Content Updating Schedule*" in such clauses 8.10 and 8.11 shall be deemed to be deleted for the purposes of this paragraph 2.6.

3 TQ Provider Approval and monitoring services

3.1 Without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*), the Supplier shall, following IfATE Approval:

3.1.1 provide that part of the Services referred to in the third column of Service Requirement 4 to ensure that the outcomes referred to in the first column of Service Requirement 4 are achieved; and

3.1.2 monitor the delivery by Approved Providers of the TQ (and the Approved Provider's continuing satisfaction of all of the requirements of the Provider Approval Criteria) in accordance with the monitoring arrangements set out in the Approved Assessment Strategy.[1]

3.2 Without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*) and paragraph 10.1 (*Reporting*) below, the Supplier shall notify the Authority (and provide full details of the circumstances) as soon as reasonably practicable where:

3.2.1 it reasonably believes that an Eligible Provider may not become an Approved Provider;

3.2.2 an Eligible Provider does not become an Approved Provider;

[1] These proposed arrangements should form part of the Supplier Response.

3.2.3 it reasonably believes that an Approved Provider may cease to be an Approved Provider;

3.2.4 an Approved Provider ceases to be an Approved Provider; and/or

3.2.5 the monitoring referred to in paragraph 3.1.2 reveals (and/or the Supplier otherwise becomes aware of):

(i) any failure by the Approved Provider to comply with the Approved Provider's Quality Assurance Process in the applicable Provider Contract;

(ii) any event, matter or circumstance which has had (or is reasonably likely to have) an adverse impact on Students (including as a result of an Appeal referred to in Service Requirement 8) and/or shall or may bring the T Level Programme into disrepute; and/or

(iii) any malpractice and/or maladministration on the part of the Approved Provider (including where any confidential TQ Live Assessment Materials (and/or the content of or information about such TQ Live Assessment Materials) is lost, stolen or transmitted).

3.3 The Supplier shall, as soon as reasonably practicable following the occurrence or identification of any matter referred to in paragraph 3.2, notify the Eligible Provider or Approved Provider (as the case may be) of any steps that are necessary to be taken by such Eligible Provider or Approved Provider (as the case may be) to remedy such matters and/or such failure and shall (as soon as reasonably practicable) notify the Authority (and provide full details) of such steps, together with details of the action that the Supplier will be taking to:

3.3.1 procure that the Eligible Provider or Approved Provider (as the case may be) takes such steps; and/or

3.3.2 mitigate the effects of such failure and/or matters.

3.4 The Supplier shall:

3.4.1 use all reasonable endeavours to procure that the Eligible Provider or Approved Provider (as the case may be) takes the steps referred to in paragraph 3.3; and

3.4.2 take the action referred to in paragraph 3.3,

together with, in either case, such further steps and/or action as the Authority may reasonably require following the notification referred to in paragraph 3.3.

3.5 The Supplier shall (in such manner (including as to timing) as the Authority may reasonably require) keep the Authority updated as to:

3.5.1 the progress by the Eligible Provider or Approved Provider (as the case may be) with the taking of the steps referred to in paragraph 3.3 (including (where applicable) whether the event, matter or circumstance giving rise to the requirement for the taking of such steps has been (or is reasonably likely to be) remedied); and

3.5.2 the action that the Supplier is taking and has taken in accordance with paragraph 3.4,

provided always that where the Supplier fails to comply with its obligations in paragraphs 3.2 to 3.4 (inclusive), such failure shall (notwithstanding the provisions of clauses 14.2.1 to 14.2.10 (*What may happen if there are issues with your provision of the Services*)) be deemed to give rise to a right for the Authority to issue written notification of Designated Action to the Supplier, to which the provisions this Contract (including clause 14.2 (*What may happen if there are issues with your provision of the Services*)) shall apply.

4 TQ Provider support services

4.1 Without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*) and Schedule 4 (*Co-operation*), the Supplier shall, throughout the Term, provide that part of the Services referred to in, and in accordance with, the third column of Service Requirement 5 to:

4.1.1 ensure that the outcomes referred to in the first column of Service Requirement 5 are achieved; and

4.1.2 following achievement of IfATE Approval, facilitate the implementation by Providers of the TQ in accordance with the Approved TQ Specification.

4.2 The Supplier shall, subject always to clause 4.12 and 4.13 (*Pricing and payments*), in respect of:

4.3 the Fees for the first Academic Year for the first Exclusive Cohort, make available details of the Fees to Eligible Providers and Approved Providers as soon as reasonably practicable;

4.4 the Fees for the second Academic Year, make available details of the Fees to Eligible Providers and Approved Providers no later than 30 April prior to the start of the second Academic Year; and

4.5 the third and each subsequent Academic Year, publish details of the Fees to Approved Providers no later than 30 April prior to the start of the relevant Academic Year.

5 Student registration and Student entry

5.1 The Supplier shall procure that Approved Providers have processes in place (and implement such processes) to ensure that, on or prior to the relevant date specified on the Key Dates Schedule for the relevant Academic Year, each Student is correctly registered for the TQ and in the manner contemplated by Service Requirement 6.

5.2 The Supplier shall procure that Approved Providers have processes in place (and implement such processes) to ensure that, on or prior to the relevant date specified on the Key Dates Schedule for the relevant Academic Year, each Student is correctly entered for assessment in respect of:

5.2.1 the TQ Core Component; and

5.2.2 each Occupational Specialist Component,

for which they are undertaking assessment.

5.3 The Supplier shall, following a request from an Approved Provider, provide the Additional Services referred to as “Late entry or entry amendment”, “Late registration or registration amendment”, “Very late entry or entry amendment” or “Very late registration or registration amendment” (as the case may be) in accordance with the applicable requirements set out against that Additional Service in Annex 10 (*Additional Services*) to this Service Requirements.

5.4 Without prejudice to the Supplier’s obligations in clause 3.1 (*How the Services must be supplied*) and paragraph 10.1 (*Reporting)* below, the Supplier shall ensure that, following IfATE Approval and (as applicable) in each Contract Month throughout the remainder of the Term, details of the registrations and assessment entries referred to in paragraph 5.1 and 5.2 are reported to the Authority in the Management Information

that is provided in respect of the Contract Month in which such registrations and/or entries are made, such reports to meet the requirements set out in the third column of each of Service Requirement 6 and Service Requirement 9 to ensure that the outcomes referred to in the first column of each of Service Requirement 6 and Service Requirement 9 are achieved.

5.5 Without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*) and elsewhere in this Service Requirements, the Supplier shall, as soon as reasonably practicable after:

5.5.1 becoming aware of any Approved Provider that is not registering any Students for the TQ (as contemplated by paragraph 5.1) and/or not entering Students for assessment (as contemplated by paragraph 5.2); and/or

5.5.2 becoming concerned as to the number of Students being registered for the TQ and/or being entered for assessment,

notify the Authority (together with full details) of such matter and/or concern.

6 TQ live assessment design and delivery

6.1 The Supplier shall (without prejudice to its obligations in clause 3.1 (*How the Services must be supplied*)):

6.1.1 on or prior to the relevant date specified on the Key Dates Schedule for the relevant Academic Year, design, develop and make available to Approved Providers the TQ Live Assessment Materials;

6.1.2 during the period specified on the Key Dates Schedule for the relevant Academic Year, administer the delivery by the Approved Providers of the TQ Live Assessment Materials and mark (or (where applicable) procure the marking and/or Moderation of) Student assessment evidence generated by the application and/or use (as the case may be) of such TQ Live Assessment Materials; and

6.1.3 during the period specified on the Key Dates Schedule for the relevant Academic Year and following a request from an Approved Provider, administer the delivery by that Approved Provider of the TQ Live Assessment Materials in respect of the Additional Services referred to as "Retakes" in accordance with the applicable requirements set out against that Additional Service in Annex 10 (*Additional Services*) of this Service

Requirements and mark (or (where applicable) procure the marking and/or Moderation of) Student assessment evidence generated by the application and/or use (as the case may be) of such TQ Live Assessment Materials,

in each case, in accordance with the then current Approved Assessment Strategy, subject to paragraph 6.2, the then current Approved Guide Standard Exemplification Materials or Grade Standard Exemplification Materials (as the case may be) and the requirements set out in the third column of Service Requirement 2 so as to ensure that the outcomes referred to in the first column of Service Requirement 2 are achieved.

6.2 The Supplier shall:

6.2.1 in respect of the First Teach Cohort for the relevant element of the Occupational Specialist Component, require the implementation and use by Approved Providers (including any assessors employed or engaged by any such Approved Provider and any Moderators where permitted in accordance with the Approved Assessment Strategy) and Assessors of the Approved Guide Standard Exemplification Materials for the purposes of assessing each Student's performance in respect of the TQ Live Assessment Materials; and

6.2.2 following grading of Student performance in respect of the TQ Live Assessment Materials undertaken by the First Teach Cohort of the relevant element of the Occupational Specialist Component and for each subsequent Cohort, develop, make available and require the implementation and use by Approved Providers (including any assessors employed or engaged by any such Approved Provider and any Moderators where permitted in accordance with the Approved Assessment Strategy) and Assessors of the Grade Standard Exemplification Materials.

6.3 The Supplier shall provide a copy of the TQ Live Assessment Materials to the Authority as soon as reasonably practicable following the date on which such TQ Live Assessment Materials are first made available to Students.

7 TQ grade awarding

7.1 Following completion of the live assessments referred to in paragraphs 6.1.2 and 6.1.3 (*TQ live assessment design and delivery*) in the relevant Academic Year, the Supplier shall (as soon as reasonably practicable but not later than the date specified on the Key Dates Schedule for the relevant Academic Year for such live assessments for that

Academic Year) assign a grade to each Student (to reflect the relevant marks awarded to each such Student) in respect of their performance in the assessment for the TQ Core Component and each Occupational Specialist Component that each such Student has undertaken in accordance with the requirements set out in the third column of Service Requirement 3 and so as to ensure that the outcomes referred to in the first column of Service Requirement 3 are achieved.

8 TQ results

8.1 The Supplier shall (as soon as reasonably practicable following completion of its obligations in paragraph 7.1 (*TQ grade awarding*), but not later than the date specified on the Key Dates Schedule for the relevant Academic Year), provide the results for each Student in the Cohort to the Authority or to the Authority's nominee (as notified by the Authority to the Supplier from time to time) in accordance with paragraph 8.2, such results to include details of:

8.1.1 the mark and grade awarded for the TQ Core Component;

8.1.2 the mark and grade awarded for each Occupational Specialist Component; and

8.1.3 such information and/or data as is required (including grade boundaries) by the Authority to award an overall grade for the T Level,

in each case, in respect of each TQ assessment that the relevant Student has undertaken.

8.2 Without prejudice to the Supplier's obligations in clause 3.1 (*How the Services must be supplied*) and paragraph 10.1 (*Reporting*) below, the Supplier shall ensure that the results referred to in paragraph 8.1 are provided to the Authority or to the Authority's nominee (as notified by the Authority to the Supplier from time to time) and reported to the Authority in the Management Information that is provided in respect of the Contract Month in which such results are required to be provided in accordance with paragraph 8.1, such results and report to meet the requirements set out in the third column of each of Service Requirement 7 and Service Requirement 9 to ensure that the outcomes referred to in the first column of each of Service Requirement 7 and Service Requirement 9 are achieved.

8.3 The Supplier shall (on the date specified on the Key Dates Schedule for the relevant Academic Year) provide to the Approved Provider a breakdown of attainment to allow

any Approved Provider and/or Student to make informed decisions about applications for (amongst other things) marking reviews and/or appeals (including a Review of Marking and/or Appeal as referred to in Annex 10 (*Additional Services*) to this Service Requirements), such breakdown (subject always to the provisions of clauses 13.10 to 13.12 (*Intellectual Property Rights*) (inclusive)) to be presented in such manner and/or format as shall not be capable of being regarded, interpreted and/or represented as a formal qualification certificate or statement of achievement.

9 TQ Post-Results Services

9.1 The Supplier shall, following the provision of the results referred to in paragraph 8.1 (*TQ results*) and, in respect of each Cohort, for a period expiring at the end of 2 Academic Years following the end of the final Academic Year for each such Cohort:

9.1.1 respond to enquiries about results; and

9.1.2 following a request from an Approved Provider made in accordance with the applicable Key Dates Schedule(s) referred to in paragraph 9.2, provide the relevant Additional Services requested by that Approved Provider (other than the Additional Services referred to in paragraph 5.3 (*Student registration and Student entry*) and 6.1.3 (*TQ live assessment design and delivery*), to which the provisions of those paragraphs shall apply) in accordance with the applicable requirements set out against the relevant Additional Services in Annex 10 (*Additional Services*) to this Service Requirements, (including as referred to in, and in accordance with, the third column of Service Requirement 8 to ensure that the outcomes referred to in the first column of Service Requirement 8 are achieved).

9.2 The Parties acknowledge and agree that the time period within which an Approved Provider may request the provision of the Additional Services referred to in paragraph 9.1.2 in relation to a Student that has undertaken an assessment (including an assessment that is a "Retake", as referred to in Annex 10 (*Additional Services*)) in an assessment series (the "**Relevant Assessment Series**") shall be as set out in the Key Dates Schedule(s) for the relevant Academic Year(s) applicable to the Relevant Assessment Series (including any Key Dates Schedule applicable to and/or regulating the provision of Additional Services in respect of assessments undertaken in the Relevant Assessment Series), provided always that nothing in this paragraph 9.2 shall operate to:

9.2.1 prevent or restrict (or be deemed to give rise to a right of the Supplier to prevent or restrict) any "Retakes" from being undertaken (or from being requested to be undertaken) in accordance with paragraph 6.1.3; and/or

9.2.2 extend the period referred to in paragraph 9.1.

10 Reporting

10.1 The Supplier shall (without prejudice to its obligations in clause 3.1 (*How the Services must be supplied*)) in each Contract Month throughout the Term, report to the Authority in accordance with (and provide such information as is required by) the requirements set out in the third column of Service Requirement 9 to ensure that the outcomes referred to in the first column of Service Requirement 9 are achieved.

11 Overarching services

11.1 The Supplier shall:

11.1.1 maintain, update and provide to the Authority (as required by clause 5.5.1 and paragraph 3.1 of Schedule 15 (*Monitoring of Performance*)) each of the Risk Register and the Issues Log;

11.1.2 implement, carry out and complete such steps (and within such time) as the Authority shall reasonably require arising out of the review of the Risk Register and/or the Issues Log pursuant to clause 5.5.1 (*Developing the TQ and achieving IfATE Approval*) and paragraph 3.1 of Schedule 15, (*Monitoring of Performance*) provided always that where the Supplier fails to implement, carry out and complete such steps in accordance with such requirements (including within such time), such failure shall (notwithstanding the provisions of clauses 14.2.1 to 14.2.10 (*What may happen if there are issues with your provision of the Services*)) be deemed to give rise to a right for the Authority to issue written notification of Designated Action to the Supplier, to which the provisions of this Contract (including clause 14.2 (*What may happen if there are issues with your provision of the Services*)) shall apply.

11.2 The Supplier shall provide all of the back-office systems and business processes necessary to enable the delivery of the Services, including IT systems, data security systems, accounting and administrative services.

11.3 The Supplier shall:

11.3.1 actively promote the T Level for which it is the TQ provider, coordinated in partnership with, and with the Approval of, the Authority; and

11.3.2 adhere to the Authority's guidelines in respect of all publicity and marketing material produced by the Supplier (or its Subcontractors) in relation to the T Level for which it is the TQ provider.

11.4 The Supplier shall, following any reasonable request from the Authority:

11.4.1 participate in and support any promotional activities intended to increase the uptake of T Levels by Providers and/or Students; and

11.4.2 without prejudice to its obligations in Schedule 4 (*Co-operation*) and Schedule 15 (*Monitoring of Performance*), attend and participate in any such meetings as the Authority may reasonably convene from time to time in connection with the T Levels Programme.

12 Efficiency

NOT USED

13 Social Value Commitments

13.1 The Supplier must ensure it takes reasonable measures to meets its Social Value commitments, in full compliance with its response to Q9.6 of the Award Questionnaire in their tender submission.

Part 2 - Service Definition Table

This Part 2 sets out the outcomes each Service must deliver and the minimum requirements the Supplier must meet when delivering each Service.

Service Requirement 1: Designing, developing and managing TQ content		
Outcomes The Specification of Content is sufficiently clear and appropriately detailed to ensure Approved Providers can properly prepare Students for the TQ assessments. The knowledge, understanding, skills and behaviours specified in the Former Supplier's TQ Specification and, if relevant, the Outline Content in relation to the TQ Core Component are up-to-date and have been validated by employers to ensure that the TQ has continued currency among	**SR1.1** Maintenance of the Specification of Content	1 **During the Initial Development, any removal of TQ Specification material from the Specification of Content must be justified and validated by a sufficient and representative sample of Employers.** Where the Supplier considers that it is necessary to remove content present in the existing TQ Specification, it shall provide a clear and detailed rationale as part of its Assessment Strategy included with the Submission for Interim Milestone 1 (and any subsequent milestones) to the Authority. Evidence from a representative sample of employers relevant to the sector must also be provided to support any proposals to remove any TQ Specification material from the Specification of Content. The Authority shall consider whether such content may be removed from the Specification of Content, provided always that the Authority's decision as to whether such content may be removed from the Specification of Content shall be final. 2 **During the Initial Development, the inclusion of additional material must be justified and validated by a sufficient and representative sample of Employers as agreed by the Authority.** The Supplier shall ensure that the Specification of Content does not include entirely new content, as distinct from updated content, that is not included in the existing TQ Specification, unless otherwise agreed by the Authority. Where the Supplier considers that it is necessary to include entirely new content, it shall provide a clear and detailed rationale as part of its Assessment Strategy included with the Submission for Interim Milestone 1 (and any subsequent milestones) to the Authority. Evidence from a representative sample of employers relevant to the sector must also be provided to support any proposals to remove any TQ Specification material from the Specification of Content. The Authority shall consider whether such new content may be included as part of the Specification of Content, provided always that the Authority's decision as to whether such new content may be included as part of the Specification of Content shall be final. The Supplier must show that new content must be covered at an appropriate depth for a level 3 qualification.

Employers and other end-users (including higher education providers). The knowledge, understanding, skills and behaviours specified in the Former Supplier's TQ Specification and, if relevant, the Outline Content in relation to each Occupational Specialist Component are up-to-date and ensure that the TQ has continued currency among Employers and other end-users (including higher education providers).		3 **During the delivery period the Supplier must ensure that the Specification of Content :** (a) enables accurate interpretation of the Specification of Content by Approved Providers (including to facilitate a clear and consistent understanding by Approved Providers of what is required to be taught and assessed for the TQ and to enable Approved Providers to determine (i) the level of competence required for staff who assess learning and (ii) any other physical requirements (such as facilities and hardware) integral to successful learning for the TQ); (b) supports Student progression and adaptability; (c) enables Students to achieve Occupational Entry Competence in relation to each Occupational Specialist Component; and (d) ensures that English, mathematics and digital content is integrated within the rest of the content in such manner as shall ensure such content is delivered and assessed in appropriate occupationally specific contexts. 4 **Components should follow the same structure as set out in the existing TQ Specification.** The Supplier shall not move elements of the existing TQ Specification which relate to one Component into another Component, unless otherwise agreed by the Authority. Where the Supplier considers that it is necessary to move content from one Component to another, it shall provide a clear and detailed rationale as part of its Assessment Strategy for Submission at Interim Milestone 1 to the Authority and the Authority shall consider whether such content may be moved, provided always that the Authority's decision as to whether such content may be moved shall be final. 5 **The TQ has two types of Component.** The Supplier shall ensure that: (e) the TQ has only two types of Component and is **not** unitised any further, such that only the TQ Core Component and each Occupational Specialist Component are formally graded;

		(f) the **TQ Core Component** clearly assesses the core knowledge, understanding, skills and behaviours relevant to all occupations within the T Level; and (g) each **Occupational Specialist Component** clearly assesses the occupationally specific knowledge, understanding, skills and behaviours relevant to the occupations within the T Level. 6 **The TQ must not be biased towards any Occupational Specialist Component.** Where there is more than one Occupational Specialist Component for the TQ, the Supplier shall ensure that the TQ Core Component is not biased towards any particular Occupational Specialist Component. This is to ensure fairness for all Students, to support learning in their chosen Occupational Specialist Component. 7 **The TQ and its Components must be appropriately titled**. The Supplier shall ensure that the TQ and the Components reflect the titling conventions in the Former Supplier's TQ Specification and, if relevant, the Outline Content. The Supplier shall agree any amendments to the titling conventions of the TQ with the Authority and shall then use only this agreed title to refer to the TQ. 8 **The Specification of Content must support fair access to attainment, including for Students with special educational needs and/or disabilities.** Without prejudice to the Supplier's obligations in clause 3.1.7 (*How the Services must be supplied*) and clause 32 (*Equality, diversity, human rights and anti-slavery*), the Supplier shall comply with all applicable Law and shall ensure that the Specification of Content is inclusive, including providing for Reasonable Adjustments and Special Consideration (as defined in SR 2.4 and SR 2.5 (respectively) below). The Supplier shall provide evidence that it has considered and addressed all such applicable Law relating to delivery of fair access to the TQ. 9 **Set recommended Guided Learning hours for each part of each Component.** The Supplier shall ensure that the Specification of Content details the recommended Guided Learning hours for each part of the TQ Core Component and each Occupational Specialist Component, including the recommended Guided Learning hours for both delivery and assessment of each such part of each such Component, provided that (i) such recommended hours are between a minimum of 900 hours and a maximum of 1400 hours and (ii) the maximum number of hours within the recommended range for the TQ Core Component are no more than 50%, and no

			less than 20%, of the overall time for the TQ. The Supplier shall provide a clear and detailed rationale for such recommended Guided Learning hours as part of its Assessment Strategy included with the Submission for the Final Approval Milestone to the Authority, or earlier at the Authority's request, and the Authority shall consider whether such proposed recommended Guided Learning hours may be included as part of the Specification of Content, provided always that the Authority's decision as to whether such recommended Guided Learning hours may be included as part of the Specification of Content shall be final. 10 **Combination of Occupational Specialist Components.** Where a T Level features more than one Occupational Specialist Component these should be specified as options from which a Student will typically select one Occupational Specialist Component. Where a Student is required to study two Occupational Specialist Components, the Supplier shall specify any prohibited combinations of Occupational Specialist Components, for example where there is overlap between the Occupational Specialist Component content or where there would be insufficient time to study a particular combination. The Supplier shall make it clear that Approved Providers can select the Occupational Specialist Component(s) they wish to deliver within these rules. Where rules of combination are given, the Supplier shall provide a clear and detailed rationale as part of its Assessment Strategy for Submission at Interim Milestone 1 which explains how any combinations are compatible and achievable within the duration of the TQ. 11 Where, in exceptional circumstances, the Supplier proposes to give Students the option to study more than two Occupational Specialist Components, it must provide a clear and detailed rationale as part of its Assessment Strategy for Submission at Interim Milestone 1 to the Authority and the Authority shall consider whether such rules of combination are appropriate, provided always that the Authority's decision as to whether such rules of combination are appropriate shall be final.
Service Requirement 2: Assessment design and delivery			
Outcomes The TQ provides for optimal assessment and reliable evidence	**SR 2.1** Assessment quality	1	The Supplier shall ensure that: (a) the Scheme of Assessment, the TQ Specimen Assessment Materials and the TQ Live Assessment Materials provide the optimum balance of the assessment principles set out below; and

of a Student's attainment in relation to the knowledge, understanding, skills and behaviours specified in the Former Supplier's Specification of Content and, if relevant, the Outline Content. The TQ supports fair access to attainment for all Students who take the TQ.		(b) the Assessment Strategy sets out a detailed rationale to explain how the TQ Specification, the TQ Specimen Assessment Materials and the TQ Live Assessment Materials meet these assessment principles. **Assessment principles** 1 **Validity.** The extent to which the TQ assessments (including the TQ Specimen Assessment Materials and the TQ Live Assessment Materials) effectively measure what they are intended to measure. This includes the extent to which TQ assessments (including the TQ Specimen Assessment Materials and the TQ Live Assessment Materials) allow Students to produce assessment evidence for the TQ that clearly corresponds to the Specification of Content and ensures the Specification of Content is not under-represented or misrepresented. 2 **Reliability.** This is about consistency and so concerns the extent to which the various stages in the TQ assessment process generate outcomes that would be replicated were the assessment repeated. The reliability of an assessment is affected by a range of factors, such as the sampling of assessment tasks and inconsistency in marking by human assessors. Reliability is critical to ensuring standards of attainment are equivalent over time (comparable performance). 3 **Comparable performance.** The extent to which the same grade for a Component with the same title indicates a comparable level of Student performance across Approved Providers (nationally) and over time. 4 **Minimising bias.** Ensuring that a TQ assessment (including the TQ Specimen Assessment Materials and the TQ Live Assessment Materials) does not produce unreasonably adverse outcomes for Students who share a particular characteristic. The Supplier should seek to ensure all Students are treated fairly and the assessment (including the TQ Specimen Assessment Materials and the TQ Live Assessment Materials) complies with all applicable Law. 5 **Minimising malpractice.** Ensuring the TQ design (including the TQ Specimen Assessment Materials and the TQ Live Assessment Materials) and processes relating to the delivery of the TQ assessments limit malpractice, including attempts by candidates to communicate with each

		other during an assessment and failures by Provider staff to comply with Supplier instructions regarding storage of Student assessment evidence. 6 **Appropriate demand.** This relates to the level of difficulty of a TQ assessment task (including within the TQ Specimen Assessment Materials and the TQ Live Assessment Materials) and the requirements of the relevant part of the Specification of Content which is to be assessed and any expectations of performance at specified grades. Demand should be appropriate to a level 3 qualification. 7 **Manageability.** The feasibility of carrying out the TQ assessment processes. A manageable assessment process is one that has reasonable expectations of Students, Approved Providers and (where appropriate) Employers. This will be based on the impact of the assessment process on Students, Approved Providers and (where appropriate) Employers as against the usefulness of the outcomes.
	SR 2.2 General assessment delivery requirements	The Supplier shall: 1 specify when the TQ assessments can be undertaken during the relevant Academic Year (taking into account any dates prescribed by the Key Dates Schedule for the relevant Academic Year) so that Students have sufficient time to generate assessment evidence and/or demonstrate the required knowledge, understanding, skills and behaviours; 2 notwithstanding the number of Assessors (and Moderators where permitted in accordance with the Approved Assessment Strategy) identified in the Implementation and Delivery Plan and/or the Resource Plan, ensure a sufficient number of qualified and trained Assessors (and such Moderators) are available to assess Students' assessment evidence for the TQ; 3 train Assessors (and Moderators where permitted in accordance with the Approved Assessment Strategy) so that their judgements in relation to the TQ assessments are consistent and accurate and applied in line with the standards defined by or through such training;

		4 sample the marking of live TQ assessments (to ensure accuracy and consistency) and, where such marking is not accurate and/or consistent, take all such steps as are necessary to ensure that such marking is accurate and consistent; 5 ensure the TQ Live Assessment Materials are made available to Approved Providers in English (online and/or in hard copy (as applicable)); 6 ensure the TQ Live Assessment Materials are available at the right time (online and/or in hard copy (as applicable)) in accordance with this Contract; 7 ensure that TQ Live Assessment Materials are free from errors and where any errors are identified in the TQ Live Assessment Materials they are dealt with appropriately, including through the issue of an erratum and by taking all such actions as are necessary to ensure that Students are not disadvantaged as a result of such errors; 8 where Student assessment evidence for the TQ is required to be generated under supervised conditions: (a) ensure that the nature of the supervised conditions and the hours for such supervised conditions are detailed in the TQ Specification; and (b) provide a clear and detailed rationale as part of its Assessment Strategy for Submission at Interim Milestone 4 to the Authority and the Authority shall consider whether such hours are appropriate, provided always that the Authority's decision as to whether such hours are appropriate shall be final; 9 ensure that Approved Providers comply with the Approved Provider's Quality Assurance Process, including: (a) keeping Students' assessment evidence for the TQ secure during and after assessment; and (b) verifying that a Student's assessment evidence for the TQ has been solely produced by that Student;

		10 following IfATE Approval, monitor the delivery of the TQ to identify any feature which could disadvantage a group of Students who share a particular characteristic and shall, as soon as reasonably practicable following identification of such a feature, take such steps as are necessary to minimise the feature being an unnecessary barrier to Student attainment; 11 monitor and investigate instances of malpractice and/or maladministration relating to the TQ in accordance with paragraph 3 (TQ Provider Approval and monitoring services) of Part 1 of this Service Requirements; 12 ensure final marks awarded by Assessors (and Moderator final marks and/or judgements, where permitted in accordance with the Approved Assessment Strategy) in relation to the TQ are collected for each Student and checked for accuracy by the relevant date specified in the Implementation and Delivery Plan; and 13 where marking is to be applied to Student assessment evidence for the TQ by Assessors (and/or by assessors employed or engaged by Approved Providers and/or Moderation is to be undertaken in relation to such marking (in circumstances where the Approved Assessment Strategy allows for use of assessors employed or engaged by the Approved Provider)), ensure: (a) such Assessors (and assessors and Moderators) are appropriately trained and competent; (b) such Assessors (and Moderators) have no personal interest in the outcome of the marking; and (c) marking and Moderation is conducted in a way which secures the accuracy of marking and a consistent approach to marking, provided always that where the Supplier determines that such marking and/or Moderation is not being undertaken accurately and consistently, it shall correct any inaccuracies and/or inconsistencies and shall take (or shall (where necessary) procure that the relevant Approved Provider and/or Moderator shall take (as the case may be)) all necessary steps to prevent any future recurrence of such inaccuracy and/or inconsistency.
	SR 2.3	1 The Supplier shall ensure that it has all necessary processes in place to ensure that, where TQ Live Assessment Materials are confidential (including the content of or information about

	Confidentiality of TQ Live Assessment Materials	such TQ Live Assessment Materials), all such TQ Live Assessment Materials remain confidential. 2 If, notwithstanding the processes referred to above, a breach of confidentiality in relation to the TQ Live Assessment Materials does occur (including through the loss, theft or transmission of confidential TQ Live Assessment Materials) or is either suspected by the Supplier or alleged by any other person (and where there are reasonable grounds for that suspicion or allegation), such matter shall be notified to the Authority in accordance with paragraph 3.2 of Part 1 of this Service Requirements and the provisions of paragraphs 3.3 to 3.5 (inclusive) of such Part 1 of this Service Requirements shall apply.
	SR2.4 Reasonable Adjustments	"**Reasonable Adjustments**" means such adjustments to and/or exemptions from the TQ Live Assessment Materials (as applicable) as are necessary and reasonable (in the context of what is being assessed) to enable a Student with special educational needs and/or disabilities to demonstrate his or her knowledge, understanding, skills and behaviours to the level of attainment required. The Supplier shall: 1 have in place clear arrangements for making Reasonable Adjustments; 2 explain (in the Assessment Strategy) how Reasonable Adjustments will be made to support fair access to attainment; and 3 provide details of such arrangements to Approved Providers, in each case, taking into account and (where applicable) implementing the process, approach and/or system agreed between the T Level Awarding Organisations pursuant to paragraph 2.1.8 of Schedule 4 (Co-operation).
	SR2.5 Special Consideration	"**Special Consideration**" means consideration to be given to a Student who has experienced a temporary illness, injury or other event outside of the Student's control and which has had, or is reasonably likely to have had, a material effect on that Student's ability to take a TQ assessment or demonstrate his or her level of attainment in a TQ assessment. The Supplier shall:

		1 have in place clear arrangements for Special Consideration; 2 explain (in the Assessment Strategy) how Special Considerations will be applied to support fair access to attainment; and 3 provide details to Approved Providers of how to request such Special Consideration, in each case, taking into account and (where applicable) implementing the process, approach and/or system agreed between the T Level Awarding Organisations pursuant to paragraph 2.1.8 of Schedule 4 (*Co-operation*).
	SR 2.6 TQ Core Component assessment design and delivery	1 **The TQ assessments must be appropriately weighted.** Where there is more than one Occupational Specialist Component for the TQ, the Supplier shall not weight the assessment of the TQ Core Component more heavily towards any one Occupational Specialist Component. This is to ensure fairness for all Students, to support learning in their chosen Occupational Specialist Component. 2 The Supplier shall assess the TQ Core Component using two distinct methods, as follows: (a) the core knowledge and understanding shall be assessed using an External Examination; and (b) the core skills and relevant aspects of core knowledge shall be assessed through the Employer Set Project in accordance with paragraph 3 below, in each case, as referred to in the Specification of Content. 3 Evidence generated by a Student in assessments of the Employer Set Project should be marked by an Assessor. However, in very exceptional circumstances set out in the Approved Assessment Strategy, an Approved Provider may be permitted to mark assessment evidence generated by a Student only where the Supplier: (i) puts in place robust arrangements which ensure that such marking achieves valid and reliable outcomes; (ii) uses an approach that is as close to complete independence as possible (such arrangements and approach to be

		detailed in the Approved Assessment Strategy); and (iii) procures that all such marking is subject to Moderation.[2] 4 **Assessment objectives.** The Supplier shall: (a) set out the assessment objectives for each of the External Examination and the Employer Set Project; and (b) specify the relevant weightings as between the External Examination and the Employer Set Project, in each case, in the Scheme of Assessment. 5 **Minimum performance requirements for the TQ Core Component must be clearly defined.** The Supplier shall ensure that: (a) the External Examination and the Employer Set Project are each assessed using compensatory assessment methods, such that high performance in one part of the TQ Core Component assessment compensates for lower performance in another; and (b) the minimum performance requirements for each judgemental grade required for the TQ Core Component shall reference each of the External Examination and the Employer Set Project. 6 **Devise the External Examination to assess the full range of knowledge and understanding outlined in the TQ Core Component.** The Supplier shall ensure that: (a) the External Examination will sample from the full breadth of relevant parts of the Specification of Content; and (b) an indicative sampling grid for the Term is included within the Assessment Strategy.

[2] These proposed arrangements should form part of the Supplier's Response.

		7 **Assessment of core skills and relevant aspects of knowledge through Employer Set Project.** The Supplier shall develop briefs for Employer Set Projects and shall ensure that: (a) such briefs are developed in collaboration with Employers; (b) each such brief enables a Student to demonstrate core skills and relevant aspects of core knowledge in an occupationally relevant context; and (c) the Assessment Strategy outlines how such briefs will continue to be relevant to the TQ Core Component throughout the Term and how the Supplier will ensure that such Employer Set Projects do not become predictable and how they will keep pace with the needs of industry, in each case, so that new briefs for Employer Set Projects are made available by the Supplier in each Academic Year. 8 **Engage with relevant Employers to set clear project briefs**. The Supplier shall: (a) engage with Employers to ensure that sufficient project brief(s) is/are made available to enable Students to demonstrate skills across the breadth of the available Occupational Specialist Component(s), provided always that where the Supplier proposes to make available only one project brief in respect of the TQ to Students and/or proposes to utilise a project brief in respect of more than one Occupational Specialist Component, then: (i) the Supplier shall provide a detailed rationale for such proposals as part of its Assessment Strategy included with the Submission for Interim Milestone 1 to the Authority; (ii) the Authority shall consider whether such proposals are acceptable; and (iii) the Authority's decision as to whether such proposals are acceptable shall be final; (b) engage with Employers to ensure that each project brief:

		(i) has clear objectives, which align with the Specification of Content and which aim to motivate Students; (ii) requires Students to solve a real world problem; (iii) enables Students to generate sufficient assessment evidence to meet the objectives referred to in (i) immediately above; (iv) clearly sets out the arrangements and restrictions for Approved Providers to support Students in carrying out and completing the Employer Set Project; and (v) allows sufficient time to enable Students to generate sufficient assessment evidence; and (c) obtain evidence of validation from each Employer involved in setting the brief(s) that they approve such brief(s) (and the Supplier shall make available to the Authority a copy of such evidence). Evidence of employer validation must include, but is not limited to, details of the questions asked of Employers, Employer responses and how the AO addressed Employer feedback.
	SR 2.7 Occupational Specialist Component assessment design and delivery	1 **Assessment of performance outcomes**. The Supplier shall ensure that: (a) the assessment materials for each Occupational Specialist Component assess all performance outcomes detailed in the Specification of Content for that Occupational Specialist Component; and (b) so far as is reasonably practicable, each assessment is synoptic to reflect how knowledge, understanding, skills and behaviours are drawn together and implemented to develop meaningful occupationally relevant Student assessment evidence, which attests to Occupational Entry Competence, provided always that where the Supplier reasonably determines that it is not possible to assess performance outcomes synoptically, the Supplier shall provide a clear and detailed rationale as part of its Assessment Strategy for Submission at Interim Milestone 1 to the Authority and the Authority shall consider whether it is acceptable not to assess performance outcomes

		synoptically, provided always that the Authority's decision as to whether such approach is appropriate shall be final. 2 Evidence generated by a Student in assessments of each Occupational Specialist Component should be marked by an Assessor. However, in very exceptional circumstances set out in the Approved Assessment Strategy, an Approved Provider may be permitted to mark assessment evidence generated by a Student only where the Supplier: (i) puts in place robust arrangements which ensure that such marking achieves valid and reliable outcomes; (ii) uses an approach that is as close to complete independence as possible (such arrangements and approach to be detailed in the Approved Assessment Strategy); and (iii) procures that all such marking is subject to Moderation.[3] 3 **Exemplifying the expected standards of attainment**. The Supplier shall, for each Occupational Specialist Component, produce Guide Standard Exemplification Materials (which shall be validated by sufficient and representative sample of Employers and Providers as agreed by the Authority)) for the purposes of IfATE Approval and for the First Teach Cohort and, for each Academic Year following grade awarding for the First Teach Cohort, produce Grade Standard Exemplification Materials (which shall be validated by Employers before results are issued) and submitted to the Authority for agreement by no later than the end of September and published by the end of October of that Academic Year, unless otherwise agreed in writing by the Authority.
Service Requirement 3: Grading and Awarding		
Outcomes Grades awarded for the TQ Core Component and each Occupational Specialist Component	**SR 3.1**	1 The Supplier shall undertake grading and awarding in accordance with the relevant part of the Approved Assessment Strategy.

[3] These proposed arrangements should form part of the Supplier's Response.

are reliable and allow Employers and other end-users (including higher education providers) to accurately identify a Student's level of attainment and effectively differentiate their performance. The TQ supports fair access to attainment for all Students who take the TQ. The minimum pass grade standard for each Occupational Specialist Component attests to Occupational Entry Competence, meets Employer expectations, and is as close to full occupational competence as possible.		
Service Requirement 4: Provider Approval		
Outcomes Approved Providers are capable of	**SR4.1**	1 The Supplier shall receive and process applications from Eligible Providers to become Approved Providers in accordance with the relevant part of the Approved Assessment Strategy.

delivering the TQ to meet the required standards and expectations.		2 The Supplier shall (within 30 Working Days) following receipt of an application for Provider Approval from an Eligible Provider: (a) assess that Eligible Provider against the Provider Approval Criteria to determine whether such Eligible Provider satisfies all of the requirements of the Provider Approval Criteria; (b) notify that Eligible Provider of the outcome of its application; and (c) where the Eligible Provider satisfies all of the requirements of the Provider Approval Criteria, grant Provider Approval in respect of such Eligible Provider.
Service Requirement 5: Provider Support		
Outcomes Approved Providers are fully supported to plan and deliver (including to properly prepare Students for assessment) the TQ to meet the required standards and expectations.	**SR 5.1**	The Supplier shall ensure that Approved Providers are fully supported to promote, plan and deliver the TQ, including: 1 setting out in the TQ Specification and Assessment Guidance for Providers any guidance and support available to the Approved Provider in respect of the TQ, which may include guidance as to sequencing of assessment of any Component; 2 providing a telephone, email and internet facility and ensuring that sufficient, suitably trained contact staff are available to: (a) answer Approved Providers' queries regarding the Provider Services and/or the TQ (including enquiries and/or queries about results); (b) deal with complaints in relation to the Provider Services and/or the TQ; and (c) ensure that such queries and/or complaints (and any queries about the T Level Programme, including different programme elements and work placements) are directed to the relevant individual at the Supplier, the Authority or other Stakeholder (as applicable);

		3 ensuring that such training, resources and other information relating to the TQ, as is necessary to assist Approved Providers' administration and examination officers, is available, including in relation to: (a) key dates for administration of the TQ; (b) how to use any systems to upload materials; and (c) which forms should be used to enable Approved Providers to claim completion of the TQ by the relevant Student; 4 ensuring that such training, resources and other information relating to the TQ, as is necessary to assist Approved Providers' teaching and learning, is available to ensure the requirements of the TQ are clear and Students can be well prepared for assessment for the TQ, including: (a) exemplifying (through the provision of and training in relation to the application of the Guide Standard Exemplification Materials) the expected standards of performance for the TQ for the First Teach Cohort, so that the Approved Providers are able to design effective courses and have a clear understanding of the quality and standards their Students need to achieve; and (b) the development in accordance with Annex 11 to the Service Requirements, of (i) Supplementary Specimen Assessment Materials; (ii) Employer Set Project Guide Exemplar Responses; (iii) Employer Set Project Grade Exemplar Responses; and (iv) Accompanying Assessment Guidance for Providers; all of which must be suitable to be used by Approved Providers to prepare Students effectively for live TQ assessments; and (c) exemplifying (through the provision of documentation, including chief examiner and chief moderator reports, which provides an overview or analysis of Student performance and includes but is not limited to, examples of student responses to assessment questions and/or tasks) the expected standards of performance for the TQ,

		so that Approved Providers are supported in understanding how students performed at item, sub-component and component level to support future teaching and learning. 5 undertaking intermittent reviews to ensure that the support remains fit for purpose, taking account of feedback from Approved Providers and amending the support packages as necessary; 6 having in place systems and processes to monitor and report to the Authority details of Approved Provider uptake of the TQ Deliverables (and any other Products and/or documents associated with the TQ), ensuring each and every Approved Provider has accessed and is using the current version of the relevant TQ Deliverable. 7 aligning training and resources with any wider FE Professional Readiness to Deliver T Levels training and support offered by the Authority; and 8 supporting Approved Providers on agreed promotional activity, as appropriate following any reasonable request from the Authority.
Service Requirement 6: Student registration and Student entry		
Outcomes Unique identification of Students	**SR 6.1**	The Supplier shall procure that Approved Providers register each Student undertaking the TQ in a way that permits the Student to be clearly and uniquely identified.
Service Requirement 7: TQ Results		
Outcomes Accurate and complete results	**SR 7.1**	The Supplier shall ensure that all results which it issues are accurate and complete and reflect the outcome of the awarding process.

Service Requirement 8: TQ Post-Results Services		
Outcomes The TQ provides for optimal assessment and reliable evidence of a Student's attainment in relation to the knowledge, understanding, skills and behaviours specified in the Former Supplier's TQ Specification and, if relevant the Outline Content. The TQ supports fair access to attainment for all Students who take the TQ.	**SR 8.1** Assessment Review	The Supplier shall ensure a transparent and effective process for review of marks (or (where applicable) Review of Moderation (as defined in Annex 10 (*Additional Services*) to this Service Requirements) for each Component.[4]
	SR 8.2 Appeals Process	1 The Supplier shall operate an appeals process, which enables Approved Providers to appeal: (a) the results of TQ assessments undertaken by Students or (in the case of an appeal in respect of an individual Student) results of TQ assessments undertaken by that Student (including in either case the outcome of a Review of Marking and/or Review of Moderation);

[4] The proposed process should form part of the Supplier Response. This requirement will simply link to the proper implementation of that process.

		(b) any decisions regarding Reasonable Adjustments and/or Special Consideration for Students or (in the case of an appeal in respect of an individual Student) decisions regarding Reasonable Adjustments and/or Special Consideration for that Student; and (c) decisions which have resulted in action taken against that Approved Provider or (in the case of an appeal in respect of an individual Student) that Student in relation to the TQ, in either case, following an investigation into malpractice or maladministration,[5] (together or individually (as the case may be) an "Appeal"). 2 Where, as a result of an Appeal, the Supplier identifies that there is or was (as the case may be) a failure in its TQ assessment process affecting more than one Student, it shall: (a) notify the Authority of such failure (including full details of the impact of such failure); (b) identify all Students who have (or who may reasonably be expected to have) been affected by the failure; (c) correct or, where it cannot be corrected, mitigate as far as possible the effect of the failure; and (d) take all such steps as are necessary to ensure that such failure does not recur in the future, and the provisions of paragraphs 3.2 to 3.5 (inclusive) of Part 1 of this Service Requirements shall apply in respect of such failure.
Service Requirement 9: Reporting		
Outcomes Accurate and timely information and data is	**SR 9.1**	The Supplier shall ensure that the Management Information is provided to the Authority as follows. In the case of:

[5] The proposed appeals process should form part of the Supplier Responses. This requirement will simply link to the proper implementation of that process.

available throughout the Term		1	the Development Phase Report, in accordance with clause 5.5 (*Developing the TQ and achieving IfATE Approval*);
		2	the Operational Delivery Report, in accordance with paragraph 3.1 of Schedule 15 (*Monitoring of Performance*);
		3	the information and data generated pursuant to paragraph 5 of Part 1 of this Service Requirements, in accordance with paragraph 5.4 of Part 1 of this Service Requirements;
		4	the information and data generated pursuant to paragraph 8 of Part 1 of this Service Requirements, in accordance with paragraph 8.2 of Part 1 of this Service Requirements;
		5	the information and data relating to the delivery of the Additional Services in accordance with paragraphs 5.3, 6.1.3 and 9.1.2 of Part 1 of this Service Requirements, in each Contract Month; and
		6	the information and data relating to adjustment to the Fees pursuant to clauses 4.12 and 4.13 (*Pricing and payments*), in accordance with clause 4.13.1 (*Pricing and payments*).
		7	the information and data relating to the delivery of the Social Value commitments in accordance with paragraph 13.1 *(Social Value Commitments)*

Part 3 – Product Descriptions

This Part 3 sets out the Product Description for each Product.

Product	Description
Assessment Strategy	A clear and detailed explanation for how the TQ meets the outcomes/overall measures and requirements for each Service. In relation to the **design** of the TQ, the Assessment Strategy shall include details of and a clear and detailed rationale for: • how the design of the TQ will ensure compliance (including ongoing compliance) with all relevant requirements of this Service Requirements; • (i) individual assessment time for each TQ assessment, for example in terms of covering the required part of the Specification of Content effectively and balancing reliability and manageability, and (ii) combined assessment time for the different TQ assessments; • the number of marks for each individual TQ assessment, for example in terms of covering the required part of the Specification of Content effectively and balancing reliability and manageability; • how the design of the TQ will ensure appropriate compensation taking into account the requirements of SR 2.6 (5) (a) of Service Requirement 2; • the approach to differentiating for the available grade range in each case; • how Students' interests will be protected if there are changes to the Specification of Content; • the Guided Learning hours for each Component, taking into account the requirements of SR 1.1 (9) of Service Requirement 1;

Product	Description
	• if applicable, why Students have been given the option to study more than two Occupational Specialist Components; • the approach to how assessments will be structured, for example in terms of covering the required part of the Specification of Content effectively and achieving the optimum balance of the assessment principles set out in SR 2.1 of Service Requirement 2, including: o the number of tasks and assessments in the External Examination; o the number of tasks and assessments in the Employer Set Project; o the relative weightings of the External Examination and the Employer Set Project; o the number of tasks and assessments for each Occupational Specialist Component; o for Occupational Specialist Components, why it is not possible to assess performance outcomes synoptically (if applicable); and o how the Former Supplier's TQ Specification and, if relevant, the Outline Content will be covered over the life of the Contract including any proposed approach to sampling. • in very exceptional circumstances where the Supplier considers that there is justification for any assessments in relation to the Employer Set Project and/or the Occupational Specialist Components to be marked by an Approved Provider and not externally marked by an Assessor, a detailed rationale which explains why this is necessary in terms of achieving an optimum balance of the assessment principles set out in SR 2.1 of Service Requirement 2 and a detailed explanation of the approach to Moderation. Exceptional circumstances shall include the following factors: o where the assessment evidence generated by Students is likely to arise spontaneously and/or be ephemeral in nature and where this may lead to significant or insurmountable logistical difficulties in terms of the Supplier arranging to be present for every assessment; o where the assessment would require repeat measurement over an extended period of time, potentially including measurement of multiple aspects across multiple Students, rather than measurement on a single occasion and where this may lead to significant or insurmountable logistical difficulties in terms of the Supplier being present for the whole period of the assessment; o where the presence of an Assessor could significantly affect the assessment, for example because it may place undue pressure on Students and therefore undermine fairness, or could require the assessment to be designed and/or completed in an artificial way which would undermine validity; and

Product	Description
	○ where the presence of an Assessor is not possible owing to issues of sensitivity and/or confidentiality with respect to individuals required to participate in the assessment(s), provided always that the factor(s) giving rise to a claim by the Supplier of the existence of any exceptional circumstances are relevant to the content of the TQ, the risks to the validity or manageability of the assessment arising as a result of such factor(s) are significant and such factor(s) and/or risk(s) cannot be managed or mitigated without marking being undertaken by an Approved Provider; • the approach to coverage of the Former Supplier's TQ Specification and, if relevant the Outline Content, including: ○ how the Former Supplier's TQ Specification and, if relevant the Outline Content has been covered overall and in each TQ assessment; ○ how the Former Supplier's TQ Specification and, if relevant the Outline Content has been elaborated on where necessary; ○ if applicable, why it is necessary to move elements of the Former Supplier's TQ Specification and, if relevant, the Outline Content which relate to one Component into another Component; and ○ if applicable, why it is necessary to include entirely new content that is not included in the Former Supplier's TQ Specification and, if relevant, the Outline Content into the Specification of Content; • the approach to: ○ mapping of the Specification of Content in TQ Specimen Assessment Materials; ○ coverage of the Specification of Content over time; and ○ ensuring the assessments for the TQ Core Component and each Occupational Specialist Component support fair access to attainment, including the approach to Reasonable Adjustments and Special Consideration; • the assessment objectives and weightings for the External Examination and the Employer Set Project; • the approach to targeting assessment objectives in the External Examination and the Employer Set Project, and to targeting performance outcomes in each Occupational Specialist Component; • the approach to each TQ assessment, including: ○ an explanation of:

Product	Description
	▪ the range of task types to be used (e.g. multiple-choice, short answer, extended response, practical assignment) and how these will support valid assessment of the Specification of Content; and ▪ the approach to mark scheme and assessment criteria design, including for different task types, and an explanation of how resulting mark schemes and assessment criteria will support reliable application by Assessors (and any assessors employed or engaged by any Approved Provider and any Moderators where permitted in accordance with the Approved Assessment Strategy); o sample question/tasks which may be from the TQ Specimen Assessment Materials, and associated mark schemes and assessment criteria, representing the range to be used in each such TQ assessment, with commentaries explaining the approaches; o an indicative sampling grid for the External Examination; and o how the requirements of SR 2.6 (7) and SR 2.6(8) of Service Requirement 2 have been taken into account. • the approach to availability of TQ assessments, including: o when assessments will be scheduled for the External Examination, the Employer Set Project and each Occupational Specialist Component; o how the approach is appropriate, including consideration of: the amount and weight of material to be covered; the extent to which different aspects would be covered sequentially or concurrently; how coherence with the overall T Level Programme will be promoted; the need to ensure that enough time is available for sufficient learning to have taken place (including how Approved Providers will be supported so that they enter Students for a Component's assessments in an appropriate Academic Year and in an appropriate assessment series within that Academic Year, in each case, within the two-year programme for the T Level); and how the approach will support standard setting; o when the first assessment cycle will be held for the First Teach Cohort, taking into account the need to ensure that standards are set appropriately in the first Academic Year so they are appropriate to be carried forward to future assessment cycles; o arrangements for Students to retake, in full, any or all of the External Examination, the Employer Set Project and each Occupational Specialist Component; and o the type of assessment (e.g. online and/or paper-based) for the External Examination, Employer Set Project and each Occupational Specialist Component; and

Product	Description
	• quality assuring the design and development of the TQ and its component assessments in line with the requirements set out in the Service Requirements and in line with the Assessment Strategy. Taking into account the approach to availability of TQ assessments, the Assessment Strategy shall include a clear and detailed explanation of any risks that have been identified, how these will be mitigated, and how particular challenges will be addressed, including: • ensuring comparability of assessments; • minimising predictability of assessments; • ensuring security and confidentiality of assessments; and • in relation to the Employer Set Project, how the Employer Set Projects will continue to be relevant to the TQ Core Component throughout the Term and how they will not become predictable and will keep pace with the needs of industry. In relation to the **delivery** of the TQ, the Assessment Strategy shall include: • details of and a clear and detailed rationale for how the delivery of the TQ will ensure ongoing compliance with all relevant requirements of this Service Requirements; • clear details of the process for developing TQ assessment materials (including TQ Specimen Assessment Materials and TQ Live Assessment Materials), including different stages and Supplier Staff involved, how evidence regarding functioning of previous assessments is used, any differences by assessment type and item setting arrangements; • clear details of the approach to training individuals who will be responsible for setting TQ assessments and/or items, including ensuring security and mitigating any conflicts of interest; • details of the nature of and number of hours of supervised conditions that will be required to deliver the TQ; • clear details of the approach to training and standardising the approach of Assessors (and any assessors employed or engaged by any Approved Provider and any Moderators where permitted in accordance with

Product	Description
	the Approved Assessment Strategy), together with details of standardisation procedures and any wider training; • a clear and detailed explanation of how the marking processes for Student assessment evidence for the TQ will operate, including any variation between the External Examination, the Employer Set Project and each Occupational Specialist Component; • a clear and detailed explanation of the process that will be in place: o to monitor accuracy and consistency of marking by Assessors (and Moderation by Moderators where permitted in accordance with the Approved Assessment Strategy) and issuing of results, and o to take remedial action where such process does not deliver accuracy and consistency of marking (and/or Moderation by Moderators where permitted in accordance with the Approved Assessment Strategy) and/or issuing of results; • a clear and detailed explanation of how malpractice will be minimised and addressed and the approach to maintaining security and confidentiality of TQ assessments, including any differences by assessment; • a clear and detailed explanation as to how live issues during assessments for the TQ will be dealt with (i.e. where the design/delivery mitigations have failed); • a clear and detailed explanation as to how results data for each Component and the TQ will be provided to the Authority in line with the Key Dates Schedule for the relevant Academic Year; and • a clear and detailed explanation as to how each Post-Results Service (referred to in paragraph 9 (*TQ Post-Results Services*) of Part 1 of this Service Requirements) will be delivered.[6] In relation to **Eligible Providers and Approved Providers**, the Assessment Strategy shall include a summary of the proposed approach to ensuring that Approved Providers are able to prepare for and undertake the TQ assessments, together with a clear and detailed explanation of:

[6] The Supplier Response should detail the Supplier's proposals for the Additional Services. This requirement will link to the proper implementation of that part of the Supplier Response.

Product	Description
	• the approach to approving Eligible Providers as Approved Providers, in line with the Provider Approval Criteria; • the approach to ensuring that all Approved Providers have appropriate and consistent quality assurance measures in place for the delivery of the TQ and ensuring that such Approved Providers maintain ongoing compliance with those quality assurance measures; • the approach to the provision of guidance and training to Approved Providers in connection with the delivery of the TQ assessments for the Employer Set Project and the Occupational Specialist Components; • the approach to monitoring Approved Providers in relation to TQ assessments for the Employer Set Project and the Occupational Specialist Components, including how this approach will ensure that such assessments remain fit for purpose on delivery; • how Guide Standard Exemplification Materials will be produced, with input from and validated by a sufficient and representative sample of Employers and Providers as agreed by the Authority; and • how Grade Standard Exemplification Materials will be produced, and kept under review, with input from validated by a sufficient and representative sample of Employers as agreed by the Authority. In relation to **awarding**, the Assessment Strategy shall include a clear and detailed explanation of: • the technical methodology employed in the awarding process, including the Supplier Staff involved and their roles; • how the decisions from the awarding process are approved within the Supplier and the Supplier Staff involved in this; • how comparability between different versions of assessments and different types of assessment (e.g. online vs paper-based) is ensured, both where these are available at the same time and on an ongoing basis;

Product	Description
	• how comparability between any options in the TQ will be ensured; • how any evidence in relation to the comparability of the TQ with the technical education qualification element for other applicable T Levels within the same Route (including those offered by other T Level Awarding Organisations) will be used to inform decisions on standard setting; • how grades are calculated, including judgemental and arithmetic grade boundaries, aggregation of marks between the External Examination and Employer Set Project, and the use of any conversion scales; and • the approach to and range of qualitative and quantitative evidence used to inform grading and awarding decisions and the weight given to different sources, together with: o a rationale for this approach in the light of the TQ design and Cohort make-up; and o details of how this approach will be kept under review and may be adjusted, including any variation between initial standard setting and maintenance of standards, and in relation to such qualitative and quantitative evidence: o qualitative evidence shall include (for the TQ Core Component and each Occupational Specialist Component as a whole and for each TQ assessment): ▪ views of senior examiners about the quality of Student assessment evidence for the TQ; ▪ views of senior examiners about the demand of TQ assessments; ▪ performance descriptions informed by Employer views; ▪ Guide Standard Exemplification Materials and Grade Standard Exemplification Materials informed by Employer views; ▪ archive Student assessment evidence for the TQ from previous series (where applicable); and ▪ if necessary, cognate Student assessment evidence for the TQ, for example from related qualifications; and o quantitative evidence shall include (for the TQ Core Component and each Occupational Specialist Component as a whole and for each TQ assessment): ▪ mark distribution; ▪ mean mark; ▪ standard deviation;

Product	Description
	▪ item-level data, such as facility and discrimination indices; ▪ percentage of Students achieving each grade in previous series; and ▪ information about Students' prior/concurrent attainment. The Assessment Strategy shall also include an explanation as to how innovation will be appropriately tested before implementation to secure on-going compliance by the Supplier with its obligations under this Service Requirements.
Employer and Provider Engagement Strategy	A clear and detailed strategy describing the approach to engaging with, and where applicable training, Employers and Providers in relation to the design, content, delivery, assessment, validation and update of the TQ and the Services, including the approach to sharing early and/or amended drafts of all Initial TQ Deliverables and TQ Deliverables with Employers and Providers (as applicable).
TQ Specification	**Specification of Content** The Specification of Content shall set out the knowledge, understanding, skills and behaviours that Students need to learn for the TQ Core Component and each Occupational Specialist Component. The Specification of Content for the TQ Core Component and each Occupational Specialist Component must be clear and unambiguous and adequately cover (and where necessary build on) the Former Supplier's TQ Specification and, if relevant, the Outline Content (and not simply replicate it). The Specification of Content shall detail the recommended Guided Learning hours for each Component (including recommended Guided Learning hours for both delivery and assessment of each Component), taking into account the requirements of SR 1.1 (9) of Service Requirement 1. The TQ Specification will be validated by a sufficient and representative number of Employers as agreed by the Authority. **Scheme of Assessment** *TQ Core Component – External Examination – knowledge and understanding* The Scheme of Assessment shall clearly set out (in relation to the External Examination) an explanation for Approved Providers of:

Product	Description
	• the assessment objectives and their weightings; • the method and number of assessments (if more than one); • the duration of the/each assessment; • the number of marks in the/each assessment; • how and when the/each assessment will be made available; • the grades available for the TQ Core Component and that these grades are for the External Examination and the Employer Set Project in combination; and • any relevant design features for the External Examination, such as the range of different question types that will be used and any access there will be to stimulus/pre-release materials. *TQ Core Component – Employer Set Project* The Scheme of Assessment shall clearly set out (in relation to the Employer Set Project) an explanation for Approved Providers of: • the assessment objectives and their weightings; • the assessment tasks available, i.e. options; • the duration of the assessment; • the number of marks for the assessment; • how and when the assessment will be made available; • the assessment criteria that will be applied (including, in very exceptional circumstances set out in the Approved Assessment Strategy, where any assessments in relation to the Employer Set Project are to be marked by an Approved Provider and not externally marked by an Assessor, details of how marks should be allocated); • the conditions under which assessment evidence must be generated; • the forms of assessment evidence that must be retained by the Approved Provider and the expectations around this; • the grades available for the TQ Core Component and that these grades are for the External Examination and Employer Set Project in combination; and • (in very exceptional circumstances set out in the Approved Assessment Strategy, where any assessments in relation to the Employer Set Project are to be marked by an Approved Provider and not externally marked by an Assessor) details of how Moderation will be conducted.

Product	Description
	The Scheme of Assessment shall also: • specify the relevant weightings as between the External Examination and the Employer Set Project; and • outline the minimum performance requirements for each judgemental grade required for the TQ Core Component (and each judgemental grade shall reference both the External Examination and Employer Set Project). *Occupational Specialist Components* The Scheme of Assessment shall clearly set out (in relation to each Occupational Specialist Component) an explanation for Approved Providers of: • the performance outcomes and how these are mapped to the Former Supplier's Specification of Content and, if relevant, the Outline Content; • the assessment task(s) for the relevant Occupational Specialist Component; • the duration of the assessment; • the number of marks for the assessment; • how and when the TQ Live Assessment Materials will be made available; • the assessment criteria that will be applied (including, in very exceptional circumstances set out in the Approved Assessment Strategy, where any assessments in relation to the relevant Occupational Specialist Component are to be marked by an Approved Provider and not externally marked by an Assessor, details of how marks should be allocated); • the conditions under which Student assessment evidence must be generated; • the forms of Student assessment evidence that must be retained by the Approved Provider and the expectations around this; • any permissions/prohibitions with respect to different Occupational Specialist Components being taken in combination; • the grades available for the relevant Occupational Specialist Component; and • (in very exceptional circumstances set out in the Approved Assessment Strategy, where any assessments in relation to the relevant Occupational Specialist Component are to be marked by an Approved Provider and not externally marked by an Assessor) details of how Moderation will be conducted.

Product	Description
	Approved Provider's Quality Assurance Process This part of the TQ Specification shall set out details of the Approved Provider's role in quality assuring the TQ assessments, to ensure compliance by the Supplier with its quality assurance obligations in the relevant part of the Supplier Response[7], for example: • authentication – ensuring Students' assessment evidence is their own; • malpractice – for example during controlled conditions; and • any other activity required of Approved Providers by the Supplier to ensure regulatory/contractual requirements are met. **Additional Information for Approved Providers** The TQ Specification shall also clearly set out: • the Qualification Purpose; and • the prior learning requirements for the TQ (if applicable). The TQ Specification shall also clearly set out, or provide appropriate links to, information regarding: • calculating grades (e.g. aggregation and scaling); • submitting general queries; • access arrangements, Reasonable Adjustments and Special Consideration; • enquiries about results and Appeals; • retakes; and • any guidance in relation to delivery of the TQ.

[7] The proposed assurance arrangements should form part of the Supplier Response.

Product	Description
TQ Specimen Assessment Materials	The TQ Specimen Assessment Materials shall comprise examples of assessments that are representative of the approach the Assessment Strategy proposes is used in live operation and shall be produced to the same quality standard. The TQ Specimen Assessment Materials shall cover each of the following: • TQ Core Component – External Examination – sample question paper and mark scheme for the/each assessment, together with mapping to the Former Supplier's Specification of Content and, if relevant, the Outline Content and sampling approach proposed; • TQ Core Component – Employer Set Project – assessment tasks/requirements for each available option and assessment criteria; and • Occupational Specialist Component – practical assessment tasks/requirements and assessment criteria for each Occupational Specialist Component. TQ Specimen Assessment Materials for all components of the TQ will be validated by a sufficient and representative number of Employers as agreed by the Authority.
TQ Live Assessment Materials	The live assessment materials (modelled on the TQ Specimen Assessment Materials and taking into account (as applicable) performance demonstrated by previous TQ Live Assessment Materials) that are to form the basis of assessment for the TQ for the relevant Academic Year.
Exemplification Materials	**Guide Standard Exemplification Materials** Guide Standard Exemplification Materials shall include indicative 'guide' examples of Student assessment evidence which the Supplier judges would be likely to meet the minimum requirements for Occupational Entry Competence and higher grades in each Occupational Specialist Component. Guide Standard Exemplification Materials will be produced in consultation with and validated by Employers. Guide Standard Exemplification Materials must accurately portray student assessment evidence and may include, but is not limited to, the use of photographic, audio or video evidence accompanied by an explanatory commentary. **Grade Standard Exemplification Materials** Grade Standard Exemplification Materials shall include actual marked examples of Students' assessment evidence, selected after awarding, which:

Product	Description
	• have met the minimum requirements for Occupational Entry Competence and higher grades in each Occupational Specialist Component; • are produced (and reviewed on an ongoing basis) in consultation with and validated by Employers; • may be used to train Assessors (and any assessors employed or engaged by an Approved Provider and any Moderators where permitted in accordance with the Approved Assessment Strategy) to ensure that Student assessment evidence is assessed to the correct standard consistently, provided always that if the materials are used to train such Assessors (and any assessors and Moderators), the Supplier shall ensure that the spread of marks covered by the materials (including the Grade Standard Exemplification Materials) that are used for such training shall not be restricted to the grade boundaries but shall include material at a range of other marks; and • meet the requirements of SR 2.7(3) of Service Requirement 2. Student assessment evidence may include, but is not limited to, the use of photographic, audio or video evidence accompanied by an explanatory commentary.
Implementation and Delivery Plan	A detailed explanation of the Supplier's proposed approach to successfully designing, developing and delivering the TQ throughout the Term (the level of detail in respect of the whole (and each relevant part of such Term) being commensurate with the level of detail that can reasonably be expected to be known by and/or available to the Supplier from time to time in respect of such whole or part of the Term), including evidence of the achievability of the proposed approach against the TQ Critical Path Diagram. It shall present a clear and achievable overall timetable for the delivery of all of the Services. The Implementation and Delivery Plan shall include information about the Supplier's: • programme and project management approach and project expertise to develop the design, content, assessment and delivery of the TQ, including details of delivery risks and plan to mitigate such risks; • financial modelling on cost of design, development and delivery of the TQ and delivery of the Services;

Product	Description
	• approach to working with Stakeholders (including, if relevant, the T Level Panel up to Interim Milestone 1) in relation to the design, development delivery and ongoing update of the TQ and the Services (including consultation with Eligible Providers to ensure the quality of the Initial TQ Deliverables at each Milestone); • approach to working with Stakeholders and organisations associated with and/or providing advice and/or guidance in relation to Students with special educational needs and disabilities in the design, development, delivery and update of the TQ and the Services, including a process for regularly reporting on progress; • approach to sharing early and/or amended drafts of the Initial TQ Deliverables and TQ Deliverables with Eligible Providers and/or Approved Providers (as applicable), including how such documents will be shared and when; • capacity to scale up in relation to demand and in response to delivery challenges to ensure overall delivery remains on track; • ability to develop and implement innovative solutions; • approach to ensuring that Management Information is interoperable with the Authority's systems and processes during the design, development and live operation of the TQ; • proposals for efficiently supporting Providers to deliver the TQ and to answer related enquiries and address related complaints (including Post-Result Services) made by telephone, by post and by other electronic correspondence efficiently and effectively; • process for raising delays or concerns; and • details of proposed joint working between T Level Awarding Organisations (as contemplated by Schedule 4 (*Co-operation*)) to support (amongst other things) the effective and efficient delivery of the T Level Programme and to streamline administration relating to the T Levels Programme in the interests of Students and Providers. The Implementation and Delivery Plan shall evidence that the Supplier has, or will have: • IT infrastructure and systems to support the design, development, delivery and award of the TQ; • secured any relevant third party contracts to support delivery of the TQ; and • processes for the design, development, delivery and award of the TQ.
Resource Plan	A detailed explanation of the Supplier's proposed approach to resourcing to ensure performance of the Services, and the successful design, development and delivery of the TQ, which shall be in the format of the template Resource Plan issued by the Authority as part of the procurement process leading to the award of this Contract.

Product	Description
	The Resource Plan shall include detail about: • all types of resources required for delivery of the Services, including a distinction between those that will be dedicated to the TQ and those that will be used for other qualifications or business areas; • the resources that will be internal and those that will be external; • the skills and experience profiles for the required resources; • any existing skills or knowledge gaps that may exist with resources already in place and how and when additional resources will be recruited, mobilised, trained and managed; • the number of resources required (including the number of Assessors (and any Moderators where permitted in accordance with the Approved Assessment Strategy) required); • what the resources would be required to deliver and by when; • how long the relevant resources would be engaged; • processes, measures and strategies that will ensure proper, effective and resilient resourcing so that the TQ will at all times operate in accordance with the Service Requirements; • processes for keeping resource requirements under review; • the proposed approach to the recruitment (including the timescales for and number) of Assessors (and any Moderators where permitted in accordance with the Approved Assessment Strategy) which have recent relevant industry experience, including the trajectory that will be required to be maintained to meet the requirements for the provision of Assessors (and (where applicable) Moderators) under this Service Requirements; • the proposed approach to the training (including the timescales) of Assessors (and any Moderators where permitted in accordance with the Approved Assessment Strategy) which have recent relevant industry experience, including the trajectory that will be required to be maintained to meet the requirements for the provision of Assessors (and (where applicable) Moderators) under this Service Requirements; • the assessment expertise, which will be used to deliver assessment design and processes set out in the Assessment Strategy; and • the occupationally specific subject expertise needed to devise and assess Occupational Specialist Components.
Submission Issues Log	The log of issues raised by the Authority in respect of the Initial TQ Deliverables following a Submission and the Supplier's detailed description of how each such issue has been resolved.

Product	Description
Risk Register	The Supplier's register detailing any events, matters and/or circumstances which it reasonably foresees (acting in accordance with Good Industry Practice) may impact upon and/or risk the successful performance of the Services by the Supplier in accordance with this Contract (or, where the Supplier has failed to create, maintain and/or update such register, such register as would detail such events, matters and/or circumstances if the Supplier was complying with its obligations under this Contract).
Issues Log	The Supplier's log detailing any events, matters and/or circumstances which have occurred and which may impact (or have impacted) upon and/or risk the successful performance of the Services by the Supplier in accordance with this Contract (or, where the Supplier has failed to create, maintain and/or update such log, such log as would detail such events, matters and/or circumstances if the Supplier was complying with its obligations under this Contract).
Provider Approval Criteria	The Supplier's criteria for the approval of Eligible Providers to deliver the TQ which shall: • ensure that the Eligible Provider's ability to deliver the TQ to the required standards and expectations is assessed and verified; • ensure that the expertise of the Eligible Provider to deliver the TQ to the required standards and expectations is assessed and verified; • ensure that resources available to the Eligible Provider to deliver the TQ in line with the required standards and expectations is assessed and verified; • promote accessibility of the TQ to all Eligible Providers; • not impose any undue and/or overburdensome administrative, financial and/or operational requirements and/or require any change in the existing administrative, financial and/or operational aspects of an Eligible Provider's business and/or operations, in either case, which could not reasonably be expected by an Eligible Provider as being strictly necessary to deliver the TQ (having regard to the administrative, financial and/or operational aspects of the business and/or operations within which Providers (operating in the same or substantially similar business and/or operations as the Eligible Provider) operate; and • not be inconsistent with and/or lead to a breach of the requirements of clause 7.1 (*Interaction with Providers*).
Assessment Guidance for Providers	Assessment Guidance shall be produced **along with** the specimen assessment materials (SAMs) and will

Product	Description
	include guidance to ensure that Providers are fully supported to prepare students for assessment. This guidance must include information relating to each component, task or similar activity. Guidance must also include but is not limited to, information on how to prepare for and administer assessments and where applicable, how to submit assessment evidence, guidance on marking and moderation as well as any other information that is required to ensure that students and Providers are fully prepared for assessments. The content must be tailored for each series and identify and expand on the guidance given for all practical assessments. Assessment Guidance must be produced in consultation with a sufficient and representative sample of Providers.

ANNEX 1 – QUALIFICATION PURPOSE

The purpose of the level 3 TQ is to ensure Students have the knowledge, skills and behaviours needed to progress into skilled employment or higher level technical training relevant to the T Level.[8]

To achieve this, each level 3 TQ must:

- provide reliable evidence of Students' attainment in relation to:
    - the core knowledge and skills relevant to the Route and Occupational Specialist Component(s) covered by the TQ; and
    - the knowledge, skills and behaviours required for at least one Occupational Specialist Component relevant to the TQ;
- be up-to-date, ensuring the knowledge, skills and behaviours needed for the Occupations have continued currency among Employers and other end-users;
- ensure maths, English and digital skills continue to be applied where they are essential to achieve occupationally relevant outcomes;
- ensure the minimum pass grade standard for Occupational Specialist Components attests to Occupational Entry Competence, meets employer expectations, and is as close to full occupational competence as possible;
- allow end users to accurately identify Students' level of attainment and effectively differentiate their performance;
- provide a clear and coherent basis for development of suitably demanding high-quality level 3 courses, which enable Students to realise their potential;
- provide Students with the opportunity to manage and improve their own performance; and
- support fair access to attainment for all Students who take the TQ, including those with special educational needs and disabilities.

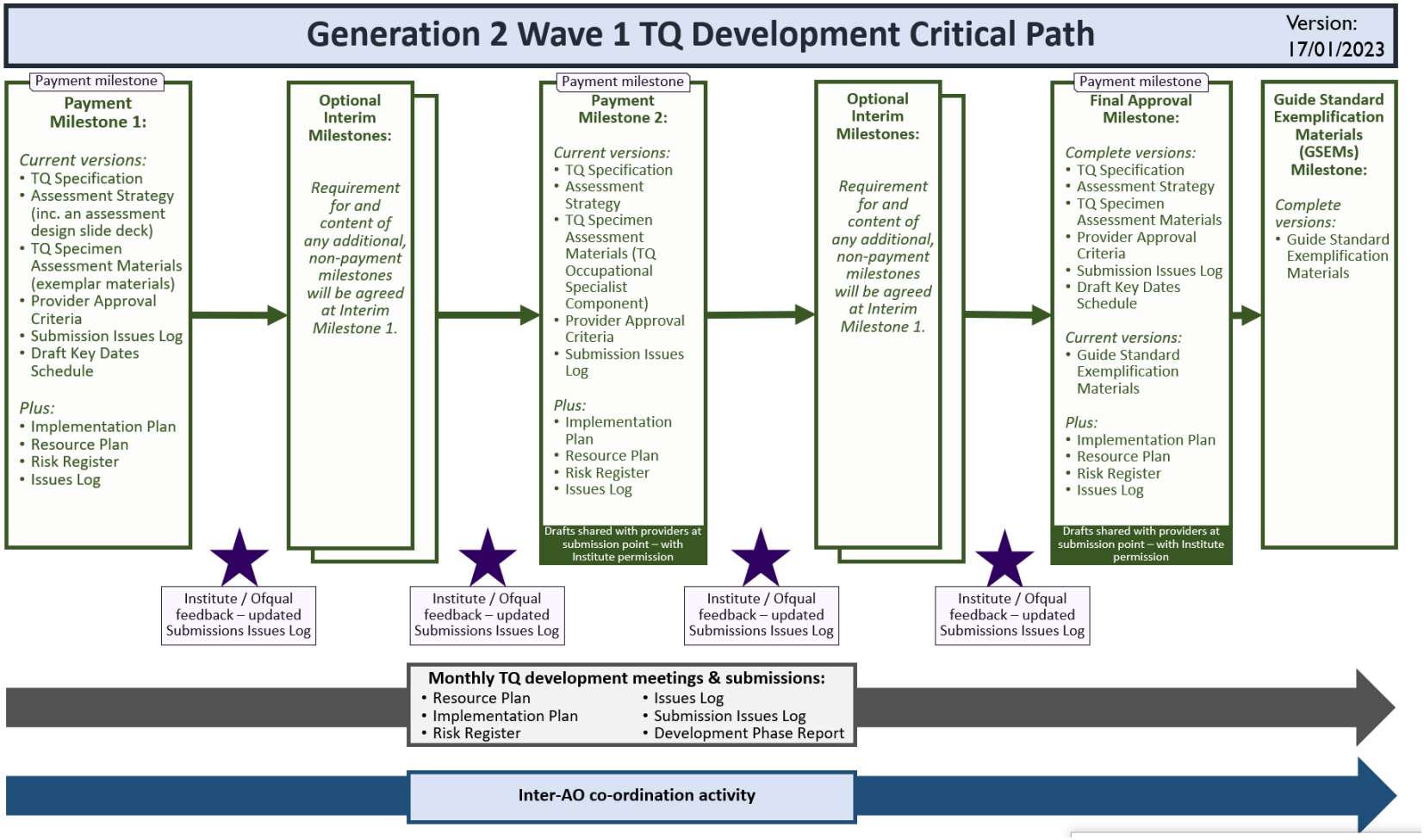
[8] The Authority may only grant IfATE Approval of the qualification "if satisfied that by obtaining the qualification a person demonstrates that he or she has attained as many of the outcomes set out in the standards as may reasonably be expected to be attained by undertaking a course of education" (sA2DA(3) of the 2009 Act).

ANNEX 2 – INTENTIONALLY BLANK

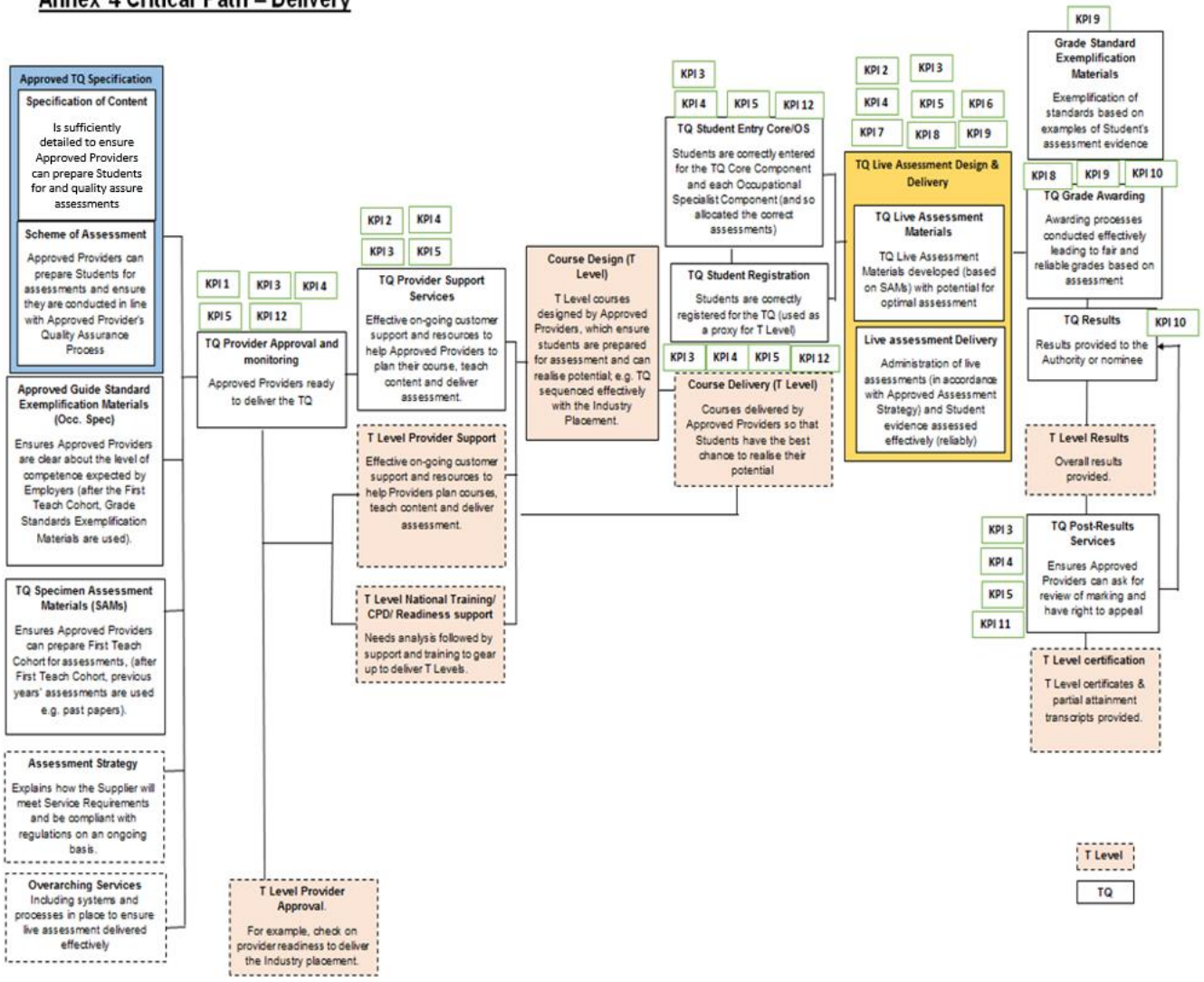
ANNEX 3 – FORMER SUPPLIER'S TQ SPECIFICATION

The TQ Specification content for this Annex is contained in a separate folder - at GEN2W1_ITT_Attachment_11_TQ_Specs

ANNEX 4 – TQ CRITICAL PATH DIAGRAM



Annex 4 Critical Path – Delivery



ANNEX 5 – INDICATIVE KEY DATES SCHEDULE[9]

To meet the requirements of Schedule 4 (*Co-operation*) the Supplier, working with other T Level Awarding Organisations, will need to produce a Key Dates Schedule, which secures the efficient and effective delivery of each assessment series for the TQ. Within the Key Dates Schedule, the deadline for submitting TQ Student registration data to the Authority must be in November in the first year of study. For a summer assessment series results must be issued on or no later than the date A level results are issued.

For a summer assessment series the key dates could include but are not restricted to:

Key Date	**Description**	**Assessment series**
November (Yr1)	Deadline for submitting TQ Student registration data to the Authority	All
3rd week Feb	Deadline for entries for assessments by Approved Providers	June
3rd week Feb	Final date for submitting Reasonable Adjustment requests to the Supplier by Approved Providers	June
4th week Feb	Assessment timetable issued	June
2nd week May	First date for submitting Special Consideration requests to the Supplier	June
2nd week May-3rd week June	Assessments take place	June
3rd week August	Restricted release of T Level results to Approved Providers by the Authority	June
3rd week August	Release of results to Students by the Authority	June

[9] This is an indicative Key Dates Schedule. Exact dates and further key dates will need to be agreed between the Supplier and other T Level Awarding Organisations through Schedule 4 (*Co-operation*) and the resulting Key Dates Schedule must be Approved by the Authority.

Key Date	Description	Assessment series
3rd week August	Release of more detailed TQ results data from the Supplier	June
3rd week September	Appeals and assessment review requests made	June
4th week Nov	T Level certificates and statements of achievement issued by the Department (or the function may be delegated to the Authority)	All

ANNEX 6 – TQ CONTENT UPDATING SCHEDULE

TQ Content Updating Schedule: Inclusive TQ Changes

Schedule Date	Activity
By end November (Academic Year X[10]-1)	Where the Authority carries out an annual review contemplated by clause 8.4, the Authority shall (where the Authority considers that the outcome of that review gives rise to any one or more Inclusive TQ Changes that the Authority requires to be implemented in accordance with this TQ Content Updating Schedule) submit to the Supplier an annual guidance note setting out such Inclusive TQ Changes.
December to February (Academic Year X-1)	The Supplier shall reflect any Inclusive TQ Changes arising out of the relevant annual guidance note (and any additional updates the Supplier proposes should be included as part of the annual review) in the Approved Initial TQ Deliverables or the TQ Deliverables (as the case may be) and/or any other Products and/or documents associated with the TQ (as applicable).
By end February (Academic Year X-1)	The Supplier shall submit the relevant Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents (as the case may be) as amended to reflect the Inclusive TQ Changes in question to the Authority for agreement.
March (Academic Year X-1)	(a) The Authority shall either: • confirm to the Supplier its agreement to the relevant amended Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents; or • notify the Supplier that the whole or part of such amended Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents are not agreed (and provide details of the comments and/or objections that the Authority has in relation to such documents). (b) The Supplier shall (as soon as reasonably practicable following receipt of the Authority's notice) make such amendments to the whole or relevant part (as the case may be) of the Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents as are necessary to address any comments and/or objections

[10] Where Academic Year X shall be the Academic Year in which the agreed amended documents reflecting the relevant Inclusive TQ Changes shall (where applicable) be implemented by Approved Providers for the new Cohort of Students.

	of the Authority and resubmit such amended documents to the Authority for agreement, to which the provisions of paragraph (a) (immediately above) shall apply.
The earlier of the end of March (Academic Year X-1) and (where applicable) the date of agreement by the Authority to the relevant amended documents	The Supplier shall make available any agreed amended Approved Initial TQ Deliverables or TQ Deliverables and (where applicable) any Products and/or documents to Approved Providers and facilitate the implementation by Approved Providers of such amended Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents, provided always that where part of any such amended document is subject to further amendment (as required by the Authority pursuant to paragraph (a) above), the Supplier shall not (unless otherwise agreed with the Authority) make any part of that relevant Approved Initial TQ Deliverable, TQ Deliverable, Product or document available to Approved Providers until the Supplier has made such amendments as are necessary to address the comments and/or objections of the Authority referred to in paragraph (a) above and the Authority has either confirmed its agreement to the resubmitted document or notified the Supplier that such document (containing only those amendments that have been agreed by the Authority) may be made available to Approved Providers.
September (Academic Year X)	Any agreed amended Approved Initial TQ Deliverables or TQ Deliverables and (where applicable) any Products and/or documents shall be implemented by Approved Providers for the new Cohort of Students.

TQ Content Updating Schedule: Exclusive TQ Changes

Schedule Date	**Activity**
End May (Academic Year X[11]-2)	Where the Authority carries out an annual review contemplated by clause 8.4, the Authority shall (where the Authority considers that the outcome of that review gives rise to any one or more Exclusive TQ Changes that the Authority requires to be implemented in accordance with this TQ Content Updating Schedule) submit to the Supplier an annual guidance note setting out such Exclusive TQ Changes.
June (Academic Year X-2) to September (Academic Year X-1)	The Supplier shall reflect any Exclusive TQ Changes arising out of the relevant annual guidance note in the Approved Initial TQ Deliverables or the TQ Deliverables (as the case may be) and/or any other Products and/or documents associated with the TQ (as applicable).

[11] Where Academic Year X shall be the Academic Year in which the agreed amended documents reflecting the relevant Exclusive TQ Changes shall (where applicable) be implemented by Approved Providers for the new Cohort of Students.

By End September (Academic Year X-1)	The Supplier shall submit the relevant Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents (as the case may be) as amended to reflect the Exclusive TQ Changes in question to the Authority for IfATE Approval.
October to November (Academic Year X-1)	(a) The Authority shall either: • confirm to the Supplier that the relevant amended Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents meet the requirements for IfATE Approval; or • notify the Supplier that the whole or part of such amended Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents do not meet the requirements for IfATE Approval (and provide details of the comments and/or objections that the Authority has in relation to such documents). (b) The Supplier shall (as soon as reasonably practicable following receipt of the Authority's notice) make such amendments to the whole or relevant part (as the case may be) of the Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents as are necessary to address any comments and/or objections of the Authority and resubmit such amended documents to the Authority for IfATE Approval, to which the provisions of paragraph (a) (immediately above) shall apply.
The earlier of the beginning of December (Academic Year X-1) and (where applicable) the date of IfATE Approval being achieved in relation to the relevant amended documents	The Supplier shall make available any amended Approved Initial TQ Deliverables or TQ Deliverables and (where applicable) any Products and/or documents that have achieved IfATE Approval to Approved Providers and facilitate the implementation by Approved Providers of such amended Approved Initial TQ Deliverables, TQ Deliverables, Products and/or documents, provided always that where part of any such amended document is subject to further amendment (as required by the Authority pursuant to paragraph (a) above), the Supplier shall not (unless otherwise agreed with the Authority) make any part of that relevant Approved Initial TQ Deliverable, TQ Deliverable, Product or document available to Approved Providers until the Supplier has made such amendments as are necessary to address the comments and/or objections of the Authority referred to in paragraph (a) above and the Authority has either confirmed that such amended resubmitted document has achieved IfATE Approval or notified the Supplier that such document (containing only those amendments on which the Authority would be prepared to award IfATE Approval) may be made available to Approved Providers.

September (Academic Year X)	Any amended Approved Initial TQ Deliverables or TQ Deliverables and (where applicable) any Products and/or documents that have achieved IfATE Approval shall be implemented by Approved Providers for the new Cohort of Students.

ANNEX 7 – INITIAL DEVELOPMENT MILESTONES

This Annex sets out the submission requirements for the three Milestones at which the Authority will render initial, interim and final payments of the Development Charge.

Further interim submission Milestones may be added to this timetable where these are agreed as part of the agreement at Interim Milestone 1. This decision will be influenced by the quantum of change to the TQ that is approved by the Authority at that initial Milestone.

In the event of any conflict and/or inconsistency between the provisions of this Annex 7 and the provisions of Annex 4 (*TQ Critical Path Diagram*) to this Service Requirements, the provisions of this Annex 7 shall prevail.

Milestone	**Submission Date**	**Submission**
Interim Milestone 1	14 October 2024 (indicative)	**TQ Specification.** A draft version of the complete TQ Specification, which takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting, and which includes: (a) a complete Specification of Content for all Components which fully covers the Former Supplier's TQ Specification and, if relevant, the Outline Content and any proposed changes to the Former Supplier's Specification of Content; (b) the proposed Guided Learning hours for each Component; (c) a draft of the Scheme of Assessment which: (i) specifies the assessment objectives for each part of the TQ Core Component;

Milestone	Submission Date	Submission
		(ii) defines each assessment method to be used for each Component; (iii) specifies indicative weightings for the assessments within the Components. **TQ Specimen Assessment Materials.** Sample indicative assessment tasks, and assessment criteria/mark schemes which takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting for: (a) each part of the TQ Core Component; and (b) at least one Occupational Specialist Component. The submission must support the exemplification of the proposals within the assessment design walkthrough and include as a minimum the following: (c) exemplar questions that cover the variety of questions types and accompanying mark scheme including indicative content; (d) exemplar tasks for one example of an Employer Set Project together with an exemplar mark scheme and indicative content; and (e) exemplar tasks for one Occupational Specialist Component Assignment together with an exemplar mark scheme including indicative content.

Milestone	Submission Date	Submission
		Assessment Strategy. A draft of the Assessment Strategy, which contains a clear explanation of the structure of the assessment design and strategy for example, the proposed number of assessments and/or assessment tasks, the duration of each and the conditions under which each would be taken. For the Employer Set Project and the Occupational Specialisms, the draft of the Assessment Strategy should also set out the proposed approach to marking and how students' application of skills and knowledge will be assessed. The draft of the Assessment Strategy shall meet (so far as is reasonably practicable having regard to the timing of Interim Milestone 1) all of the requirements of the Product Description for the Assessment Strategy and take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. The Submission must include an: **Assessment design slide deck.** A slide deck which contains a clear explanation of the structure of the assessment design and explanation of the design decision rationale for the TQ Core Component and Occupational Specialist Component. The slide deck must contain the structural elements and rationale in accordance with any guidance on the Service Requirements issued by the Authority and take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. The assessment design slide deck will be used to facilitate a walkthrough with the Authority shortly following the submission. **Implementation and Delivery Plan.** A complete version of the Implementation and Delivery Plan, which meets (so far as is reasonably practicable having regard to the timing of Interim Milestone 1) all of the requirements of the Product Description for the Implementation and Delivery Plan and which also takes in account any comments, objections, recommendations

Milestone	Submission Date	Submission
		and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting **Resource Plan.** A complete version of the Resource Plan, which meets (so far as is reasonably practicable having regard to the timing of Interim Milestone 1) all of the requirements of the Product Description for the Resource Plan and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Provider Approval Criteria.** A complete version of the Provider Approval Criteria, which meets (so far as is reasonably practicable having regard to the timing of Interim Milestone 1) all of the requirements of the Product Description for the Provider Approval Criteria and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Risk Register and Issues Log.** An updated and complete version of each of the Risk Register and the Issues Log which meet all of the requirements of the Product Description for the Risk Register or Issues Log (as applicable) and which take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Submission Issues Log.** An updated Submission Issues Log which meets all of the requirements of the Product Description for the Submission Issues Log, and which explains how each issue raised by the Authority to date has been dealt with in this Submission.

Milestone	Submission Date	Submission
		Employer and Provider Engagement Strategy. A complete version of the Employer and Provider Engagement Strategy, which meets (so far as is reasonably practicable having regard to the timing of Interim Milestone 1) all of the requirements of the Product Description for the Employer and Provider Engagement Strategy and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier in respect of the Supplier's Response and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting.
Interim Milestone 2	2 December 2024 (indicative)	**TQ Specification.** a complete version of the TQ Specification, which meets all of the requirements of the Product Description for the TQ Specification and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **TQ Specimen Assessment Materials and accompanying Assessment Guidance for Providers.** A complete version of the TQ Occupational Specialist Component and each part of the TQ Core Component, and accompanying Assessment Guidance for Providers which meet all of the requirements of the Product Descriptions and which also take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Assessment Strategy.** A complete version of the Assessment Strategy, which meets all of the requirements of the Product Description for the Assessment Strategy and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting.

Milestone	Submission Date	Submission
		Implementation and Delivery Plan. A complete version of the Implementation and Delivery Plan, which meets all of the requirements of the Product Description for the Implementation and Delivery Plan and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Resource Plan.** A complete version of the Resource Plan, which meets all of the requirements of the Product Description for the Resource Plan and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Provider Approval Criteria.** A complete version of the Provider Approval Criteria which meets (so far as is reasonably practicable having regard to the timing of Interim Milestone 4) all of the requirements of the Product Description for the Provider Approval Criteria and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Risk Register and Issues Log.** A complete version of each of the Risk Register and the Issues Log which meet all of the requirements of the Product Description for the Risk Register or Issues Log (as applicable) and which also take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Submission Issues Log.** An updated Submission Issues Log which meets all of the

Milestone	Submission Date	Submission
		requirements of the Product Description for the Submission Issues Log, and which explains how each issue raised by the Authority to date has been dealt with in this Submission. **Employer and Provider Engagement Strategy.** A complete version of the Employer and Provider Engagement Strategy, which meets all of the requirements of the Product Description for the Employer and Provider Engagement Strategy and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at Interim Milestone 1 and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting.
Final Approval Milestone	14 February 2025 (indicative)	**TQ Specification**. A complete version of the TQ Specification, which meets all of the requirements of the Product Description for the TQ Specification and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **TQ Specimen Assessment Materials and accompanying Assessment Guidance for Providers.** A complete version of the TQ Specimen Assessment Materials, and accompanying Assessment Guidance for Providers which meet all of the requirements of the Product Descriptions and which also take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Assessment Strategy.** A complete version of the Assessment Strategy, which meets all of the requirements of the Product Description for the Assessment Strategy and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in

Milestone	Submission Date	Submission
		connection with the submission of such Product at any previous TQ Development Meeting. **Implementation and Delivery Plan.** A complete version of the Implementation and Delivery Plan, which meets all of the requirements of the Product Description for the Implementation and Delivery Plan and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Resource Plan.** A complete version of the Resource Plan, which meets all of the requirements of the Product Description for the Resource Plan and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Provider Approval Criteria**. A complete version of the Provider Approval Criteria, which meets all of the requirements of the Product Description for the Provider Approval Criteria and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Risk Register and Issues Log.** A complete version of each of the Risk Register and the Issues Log which meet all of the requirements of the Product Description for the Risk Register or Issues Log (as applicable) and which also take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting.

Milestone	Submission Date	Submission
		Submission Issues Log. An updated Submission Issues Log which meets all of the requirements of the Product Description for the Submission Issues Log, and which explains how each issue raised by the Authority to date has been dealt with in this Submission. **Employer and Provider Engagement Strategy.** A complete version of the Employer and Provider Engagement Strategy, which meets all of the requirements of the Product Description for the Employer and Provider Engagement Strategy and which also takes into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any previous Interim Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting. **Draft Key Dates Schedule.** An updated version of the Key Dates Schedule.
Guide Standard Exemplification Materials	February 2025 (Indicative)	**Exemplification Materials.** A complete version of the Guide Standard Exemplification Materials for each Occupational Specialist Component, which meet all of the requirements of the Product Description for the Guide Standard Exemplification Materials and which also take into account any comments, objections, recommendations and/or requirements notified by the Authority to the Supplier at any Milestone and/or arising out of or in connection with the submission of such Product at any previous TQ Development Meeting or any other feedback.

ANNEX 8 – ELIGIBLE PROVIDERS

Part 1 – Eligible Providers 2025 Cohort

The Eligible Providers for the Academic Year commencing 2025 are published on the Gov.uk website here:

https://www.gov.uk/government/publications/providers-selected-to-deliver-t-levels

Part 2 – Eligible Providers Subsequent Cohorts

The Authority shall, not later than 12 months prior to the commencement of the relevant Academic Year, notify the Supplier of the Eligible Providers for such Academic Year.

ANNEX 9 – MANAGEMENT INFORMATION

Information/ report	Description
Development Phase Report	In the period prior to IfATE Approval, the Supplier shall prepare and provide a dashboard report (in such form as the Authority may specify from time to time) summarising: • the Supplier's progress against and compliance (to date) with the Implementation and Delivery Plan (including progress against any milestones (including any Milestones)) and the Resource Plan; • how the Supplier is managing any risks and issues identified in the updated Risk Register and/or Issues Log, including the Supplier's progress against any steps required by the Authority to be carried out by the Supplier in accordance with paragraph 11.1.2 of Part 1 of this Service Requirements; • how Employers (and other end users, including higher education providers) have been consulted in relation to the design of the TQ; and • such other information as the Authority may reasonably require from time to time.

Operational Delivery Report	**Monthly Performance Report**
	
	The Supplier shall prepare and provide a dashboard report (in such form as the Authority may specify from time to time) summarising:
	
	• the Supplier's progress against and compliance (to date) with the Implementation and Delivery Plan, the Resource Plan and the Key Dates Schedule for the relevant Academic Year;
	• how the Supplier is managing any risks and issues identified in the updated Risk Register and/or Issues Log, including the Supplier's progress against any steps required by the Authority to be carried out by the Supplier in accordance with paragraph 11.1.2 of Part 1 of this Service Requirements;
	• for each KPI in respect of which the Performance Monitoring Period ends in that Contract Month:
	  ○ the actual performance achieved by the Supplier for that KPI during that Performance Monitoring Period; and
	  ○ details of any Service Failure that occurred in respect of that KPI, together with the proposed KPI Improvement Plan;

Information/ report	Description
	• details of the Supplier's progress against each KPI Improvement Plan that the Supplier is (or should be, if it was complying with its obligations under this Contract) carrying out and/or completing during the relevant Contract Month; • the Supplier's progress in carrying out any Designated Action notified by the Authority pursuant to clause 14.2 (*What may happen if there are issues with your provision of the Services*); • without prejudice to clause 14.1 (*What may happen if there are issues with your provision of the Services*), any Critical Service Failures occurring in the relevant Contract Month; • any areas of the Services (and/or the performance of the Services) where the Supplier reasonably considers that there could be innovations and/or improvements in the delivery and/or performance of the Services, including key risks and potential benefits; • progress in implementing, and the actual impact of, any innovations and/or improvements previously notified by the Supplier; • evidence demonstrating that the Supplier is achieving the overarching outcomes for each element of the Services, as set out in the first column of the Service Definitions Table; • the monitoring undertaken by the Supplier in accordance with paragraph 3.1.2 of Part 1 of this Service Requirements in the relevant Contract Month to include reporting on Provider usage of training, resources and other support materials made available by the Supplier; • any events, matters and/or circumstances referred to in paragraph 3.2 of Part 1 of this Service Requirements occurring in the relevant Contract Month, together with the progress (during the relevant Contract Month) of the Eligible Provider or Approved Provider (as the case may be) and the Supplier in taking the steps and/or actions referred to in paragraphs 3.3 and 3.4 of Part 1 of this Service Requirements; and • such other information as the Authority may reasonably require from time to time having regard to, amongst other things, the period in the Academic Year within which the relevant Contract Month falls. In relation to the assessment of the Supplier's performance against each KPI, the Supplier shall submit all such evidence as is referred to in the fifth column of the Table set out in Annex 1 to Schedule 15 (*Monitoring of Performance*), other than where such evidence is stated to be obtained via a survey. Notwithstanding the evidence that the Supplier is required to provide (referred to in the fifth column of the Table set out in Annex 1 to Schedule 15 (*Monitoring of Performance*)) to enable

Information/ report	Description

	the assessment of the Supplier's performance against each KPI, the Supplier shall also include within this Monthly Performance Report the following data and information (broken down by KPI):
	
	• KPI 1 (Provider approval and monitoring):
	  ○ the number of Eligible Providers applying to become Approved Providers, broken down into those Eligible Providers that are seeking a full approval and those Eligible Providers that are seeking to extend an existing approval;
	  ○ the number and details of Eligible Providers that have submitted an application to become an Approved Provider and who have (i) not become an Approved Provider and (ii) become an Approved Provider;
	  ○ the number and details of Eligible Providers that are awaiting a decision on their application to become an Approved Provider;
	  ○ the number and details of Eligible Providers in respect of which a decision has been made within 30 Working Days of receipt by the Supplier of the relevant application; and
	  ○ details of the actual monitoring of Approved Providers undertaken by the Supplier in the relevant Contract Month.
	• KPI 2 (Approved Provider preparedness).[12]
	• KPI 3 (Queries from Eligible Providers and Approved Providers):
	  ○ the number of letters and other forms of electronic correspondence received (broken down by letter and each other form of electronic correspondence) and number of telephone calls received, in each case, in the relevant Contract Month;
	  ○ a summary of key topics or queries being asked;
	  ○ details of the percentage of such queries being resolved within the Target Service Level (broken down by letter (and each other form of electronic correspondence) and telephone calls); and
	  ○ details of any repeat queries (including where any such queries have been raised and/or resolved in any previous Contract Month).
	• KPI 4 (Complaints):
	  ○ the number of complaints received in the relevant Contract Month;
	  ○ a summary of the nature of each such complaint;
	  ○ details of the percentage of such complaints being resolved within the applicable Target Service Level;

[12] To be measured by a survey undertaken or commissioned by the Authority.

Information/ report	Description
	○ details of why any complaints that have not been resolved within the applicable Target Service Level have not been so resolved; and ○ details of any repeat complaints or further complaints linked to a previous complaint (including where any such complaints have been made and/or resolved in any previous Contract Month). • KPI 5 (Provider satisfaction).[13] • KPI 6 (Numbers of appropriately qualified and trained Assessors (and (where applicable) Moderators)): ○ details of the actual number of Assessors (and (where applicable) Moderators) that have been recruited, trained and retained in the relevant Contract Month; and ○ details of the number of Assessors (and (where applicable) Moderators) contemplated by the relevant Contract Month (or in line with the trajectory (as the case may be)) as set out in the then current Implementation and Delivery Plan and/or Resource Plan. The Authority may require the Supplier to provide this data more frequently than monthly during the key assessment delivery period. • KPI 7 (Quality of TQ Live Assessment Materials): ○ a summary of activities completed in the relevant Contract Month relating to the development of the TQ Live Assessment Materials, as contemplated in the Assessment Strategy and/or the Implementation Plan; ○ a summary of the actual quality assurance activity undertaken by the Supplier in the relevant Contract Month; ○ a summary of the quality assurance activity (if any) that is contemplated in the Assessment Strategy as being undertaken by the Supplier in or during (as the case may be) the relevant Contract Month; and ○ details of any errors reported in the TQ Live Assessment Materials in the relevant Contract Month. • KPI 8 (Student assessment evidence assessed and processed): ○ a summary of the actual quality assurance activity undertaken by the Supplier to verify the quality of the processing of Student assessment evidence for awarding in the relevant Contract Month, together with evidence that such

[13] To be measured by a survey undertaken or commissioned by the Authority.

Information/ report	Description
	processing has been undertaken accurately and consistently; ○ a summary of the quality assurance activity (if any) that is contemplated in the Assessment Strategy as being undertaken by the Supplier to verify the quality of the processing of Student assessment evidence for awarding in or during (as the case may be) the relevant Contract Month; ○ details of the cumulative volume and percentages of Student assessment evidence processed (broken down to the TQ Core Component and each Occupational Specialist Component) by the end of the relevant Contract Month, as against the planned trajectory and dates in the Implementation and Delivery Plan applicable to that Contract Month; and ○ details of any errors, inaccuracies and/or inconsistencies identified in any processed Student assessment evidence in the relevant Contract Month. • KPI 9 (Validation of Grade Standard Exemplification Materials):[14] For each Occupational Specialism: ○ a summary of the employer validation activity undertaken to validate Grade Standard Exemplification Materials ○ the number of employers who have been involved in the validation process; including details as to whether they have been involved in the panel prior to each validation exercise ○ evidence of validation from at least 5 different Employers relevant to the Occupational Specialism that validate the Grade Standard Exemplification Materials. ○ evidence of validation from at least 5 different Employers relevant to the Occupational Specialism that the Grade Standard Exemplification Materials are comparable to the Approved Guide Standard Exemplification Materials. • KPI 10 (Student assessment results submitted by relevant date): ○ details of the cumulative volume and percentages of Student results submitted by the Supplier to the Authority (or the Authority's nominee (as applicable)) by the end of the relevant Contract Month; and

[14] To be assessed by the receipt and review by the Authority of evidence of validation from Employers in the relevant Contract Month.

Information/ report	Description
	○ details of the cumulative volume and percentages of Student results envisaged in the Implementation and Delivery Plan to be submitted by the Supplier to the Authority (or the Authority's nominee (as the case may be)) by the end of the relevant Contract Month. • KPI 11 (Post-Results Services): ○ the total volume of Post-Results Services (broken down by service) and percentage of each Post-Results Service (as against total Post-Results Services) undertaken by the Supplier in the relevant Contract Month; ○ detail of the timing of delivery of Post-Results Services against the applicable timeframes in Annex 10 (*Additional Services*) of this Service Requirements as contemplated by the Supplier's Response; and ○ detail of the proportion of remarks and Appeals which have resulted in grade increases or decreases (and summary of key reasons for any changes made). • KPI 12 (Submission of information): ○ details of the Management Information, required or requested Products including Key Materials and/ or Ancillary Materials submitted in respect of the relevant Contract Month; ○ details of the Management Information, required or requested Products including Key Materials and/ or Ancillary Materials anticipated to be submitted in respect of the relevant Contract Month; and ○ details of any errors, inaccuracies and/or inconsistencies identified in any Management Information, required or requested Products including Key Materials and/ or Ancillary Materials submitted in respect of the relevant Contract Month (and/or any previous Contract Month). **Ongoing Development Services Report** A dashboard report (in such form as the Authority may specify from time to time) summarising: • the Supplier's progress against and compliance (to date) with the TQ Content Updating Schedule (including progress against any milestones); • any proposed amendments and/or updates made to any Product during the relevant Contract Month pursuant to paragraphs 2.5 and/or 2.6 of Part 1 of this Service Requirements; and

Information/ report	Description
	• such other information as the Authority may reasonably require from time to time. **Annual Services Report** By the end of August each year, a high level overview of the Supplier's assessment of its performance during that Academic Year, summarising: • the key successes and areas for improvement in the delivery of the Services and/or the TQ; • in respect of the assessment cycles in that Academic Year, what important lessons were learned and how these will be addressed in following assessment cycles; • the key issues for the next following Academic Year; • how Employers have been consulted in relation to (and been involved in the design and delivery of) TQ assessment; • performance against the Social Value commitments under paragraph 13.1 (*Social Value Commitments*); and • (where appropriate), the preparations for handover at the end of the Term. The Supplier shall also provide an updated Exit Plan in accordance with paragraph 2 of Schedule 12 (*Exit Management*). **Annual Penetration Testing Report** By the end of August each year, a summary of: • the Supplier's findings of independent penetration testing undertaken to test the security of any IT systems and hosting environments that are used to handle, store or process IfATE Data; and • details of any necessary remedial works required as a result of such penetration testing.
Student registrations and Student entries (as referred to in paragraph 5 of Part 1 of this Service Requirements)	In relation to the Supplier's obligations in paragraph 5.4 of Part 1 of this Service Requirements, the Supplier shall report the following information and data (in a spreadsheet but in such form as the Authority may specify from time to time): • the number of Students registered for the TQ by Approved Provider (including late registrations and/or registration amendments and very late registrations and/or registration amendments (each as referred to in Annex 10 to this Service Requirements)):

Information/ report	Description
	○ in the current Academic Year; and ○ in aggregate (including for the current Academic Year) during the Term to date; • the number of Student entries by Approved Provider (including late entries and/or entry amendments and very late entries and/or entry amendments (each as referred to in Annex 10 to this Service Requirement)) in the relevant Academic Year for: ○ the TQ Core Component; and ○ each Occupational Specialist Component, together with the number of such entries in aggregate (including for the current Academic Year) for each of the TQ Core Component and each Occupational Specialist Component for all Academic Years during the Term to date; • the number of withdrawn entries in the relevant Academic Year (by Approved Provider) for: ○ the TQ Core Component; and ○ each Occupational Specialist Component, together with the number of such withdrawals in aggregate (including for the current Academic Year) for each of the TQ Core Component and each Occupational Specialist Component for all Academic Years during the Term to date; and • such other information as the Authority may reasonably require from time to time.
TQ results (as referred to in paragraph 8 of Part 1 of this Service Requirements)	In relation to the Supplier's obligations in paragraph 8.2 of Part 1 of this Service Requirements, the Supplier shall report the following information and data (in such form as the Authority may specify from time to time) to the Authority (or the Authority's nominee (as applicable)): • results for each Student for the TQ Core Component and each Occupational Specialist Component that such Student has undertaken including: ○ Unique Learner Number; ○ name of Approved Provider; ○ Supplier name; ○ details of the TQ achieved; ○ the grade awarded for each Component; ○ date of achievement; • the outcome of any Appeals, Clerical Check, Expedited Review of Marking, Review of Marking, and/or Review of Moderation (each as referred to in Annex 10 (*Additional Services*) to this Service Requirements)), including

Information/ report	Description
	details of the nature of the Appeal and a summary of the grounds for the Appeal; and • such other information as the Authority may reasonably require from time to time, to enable, amongst other things, the aggregation for T Level certification and inclusion in any Provider performance tables.
Additional Services	Data and information on the volume and nature of Additional Services being delivered to Approved Providers in the relevant Contract Month, in aggregate for the Academic Year to date and in aggregate (including for the current Academic Year) for all Academic Years during the Term to date (in spreadsheet format and in such form as the Authority may specify from time to time).
Adjustments to Fees	In advance of its publication and availability to Approved Providers and in accordance with clause 4.13 (*Pricing and payments*), proposed adjustments to the Fees for the following Academic Year. In accordance with clause 4.13 (*Pricing and payments*), proposed adjustments to the Rate Card for the following Academic Year. The information for each of the proposed adjustments to the Fees and the proposed adjustments to the Rate Card will be submitted separately in a spreadsheet format (in such form as the Authority may specify from time to time) and will include any proposed annual percentage change in each proposed Fee and each proposed rate in the Rate Card, as such proposed change shall be calculated in accordance with clauses 4.12 and 4.13 (*Pricing and payments*).

ANNEX 10 – ADDITIONAL SERVICES

Additional Service	Additional Service Requirements
Access to Student assessment evidence	The Supplier shall within 10 Working Days following receipt of a request from the relevant Approved Provider, send (in such form as such Approved Provider shall request) to that Approved Provider a copy (including, as applicable, a PDF copy) of the relevant original marked Student assessment evidence or the whole or the relevant part (as the case may be) of the original TQ Live Assessment Materials to which the Student assessment evidence relates, to help the Approved Provider (or relevant Student (as the case may be)) decide whether to request a Review of Marking or Review of Moderation (each as defined below).
Additional Approved Provider support visit	The Supplier shall, as soon as reasonably practicable following receipt of a request from an Approved Provider, attend such Approved Provider's premises and provide such additional support as such Approved Provider reasonably requires, such as support in relation to misinterpretation of the TQ Specification.
Appeal	The Supplier shall: (i) within 20 Working Days following receipt of a request from an Approved Provider for an Appeal, undertake a detailed review of all information, data and/or documents relating to the Appeal, including the assessment evidence relating to the whole or the relevant part of a Cohort or an individual Student (as the case may be); and (ii) within 20 Working Days following receipt of a request from an Approved Provider for an Appeal hearing, hold an Appeal hearing in which the Approved Provider or its representative(s) can make submissions in relation to the Appeal, including (where applicable) explaining its dissatisfaction with any grade(s) awarded in relation to the whole or any part of a Cohort or an individual Student (as the case may be), following which the Supplier shall notify the Approved Provider of the outcome of such Appeal and, where necessary, adjust the marks awarded to the whole or any part of a Cohort or an individual Student (as the case may be) and issue new results to the Authority (or its nominee (as the case may be)), provided always that this Additional Service shall only be deemed to be an Additional Service in respect of which a Fee shall be payable by the Approved Provider if, following the determination of such Appeal, the Approved Provider is not successful in the Appeal.
Clerical Check	The Supplier within 10 Working Days following receipt of a request from an Approved Provider, undertake a detailed review of the relevant Student's assessment evidence and recount all of

Additional Service	Additional Service Requirements
	the marks that such Student has been awarded to ensure that the total number of marks awarded to such Student (leading to the award of the relevant grade(s)) equal the number of marks that should have been awarded to such Student and, where necessary, adjust the marks awarded to the Student, notify the Approved Provider of such adjustment and issue new results to the Authority (or its nominee (as the case may be)).
Expedited Review of Marking	The Supplier shall within 10 Working Days following receipt of a request from an Approved Provider, undertake an expedited Review of Marking (as defined below), provided always that this Additional Service shall only be deemed to be an Additional Service in respect of which a Fee shall be payable by the Approved Provider if, following the carrying out and completion of such an expedited Review of Marking, the grade(s) awarded to such Student is not changed.
Late entry or entry amendment	Where, following the entry deadline for the TQ Core Component and/or relevant Occupational Specialist Component specified in the Key Dates Schedule for the relevant Academic Year until the very late entry deadline for the TQ Core Component and/or relevant Occupational Specialist Component specified in the Key Dates Schedule for the relevant Academic Year, an Approved Provider requires a new Student to be entered for the TQ Core Component and/or relevant Occupational Specialist Component and/or an existing entry for a Student to be amended, the Supplier shall following receipt of a request from an Approved Provider no later than 20 Working Days prior to the commencement of the relevant assessment as determined in accordance with the relevant Key Dates Schedule, enter that Student for the TQ Core Component and/or relevant Occupational Specialist Component or amend that Student's entry for the TQ Core Component and/or relevant Occupational Specialist Component (as the case may be).
Late registration or registration amendment	Where, following the registration deadline for the TQ specified in the Key Dates Schedule for the relevant Academic Year until the very late registration deadline for the TQ specified in the Key Dates Schedule for the relevant Academic Year, an Approved Provider requires a new Student to be registered for the TQ and/or an existing registration for a Student to be amended, the Supplier shall following receipt of a request from an Approved Provider no later than 20 Working Days prior to the commencement of the relevant assessment as determined in accordance with the relevant Key Dates Schedule, register that Student for the TQ or amend that Student's registration for the TQ (as the case may be).
Retake	Where, in the period following the publication of the TQ results in accordance with paragraph 8 of Part 1 of this Service Requirements until two years after the end of the final Academic Year for the Cohort within which the relevant Student is included,

Additional Service	Additional Service Requirements
	an Approved Provider requests that a Student wishes to retake all or any of the assessments for: • the TQ Core Component - External Examination; • the TQ Core Component - Employer Set Project; and/or • an Occupational Specialist Component, the Supplier shall carry out and complete its obligations in paragraphs 6.1.3 (*TQ live assessment and delivery*), 7 (*TQ grade awarding*), 8 (*TQ Results*) and 9 (*TQ Post Results Services*) (save to the extent that compliance with such obligations in that paragraph 9 (*TQ Post Results Services*) would otherwise require the performance of a further Additional Service and in respect of which the provisions applicable to that further Additional Service shall apply) in each case of Part 1 of this Service Requirements in respect of such Student.
Review of Marking	The Supplier shall within 25 Working Days following receipt of a request from an Approved Provider, undertake a detailed review of the relevant Student's assessment evidence alongside the TQ Live Assessment Materials applicable to such assessment evidence to ensure that the marking scheme has been complied with in full in relation to the marking of that Student's assessment evidence, provided always that this Additional Service shall only be deemed to be an Additional Service in respect of which a Fee shall be payable by the Approved Provider if, following the carrying out and completion of such review, the grade(s) awarded to such Student is not changed.
Review of Moderation	The Supplier shall within 25 Working Days following receipt of a request from an Approved Provider, undertake a detailed review of the relevant Cohort's assessment evidence alongside the assessment criteria within the Scheme of Assessment to ensure that the assessment criteria has been complied with in full in relation to the marking of that Cohort's assessment evidence, provided always that this Additional Service shall only be deemed to be an Additional Service in respect of which a Fee shall be payable by the Approved Provider if, following the carrying out and completion of such Review of Moderation, the grade(s) awarded to any Student is not changed.
Very late entry or entry amendment	Where, following the very late entry deadline for the TQ Core Component and/or relevant Occupational Specialist Component specified in the Key Dates Schedule for the relevant Academic Year until the date on which entries or amendments to entries finally closes for the TQ Core Component and/or relevant Occupational Specialist Component as specified in the Key Dates Schedule for the relevant Academic Year, an Approved Provider requires a new Student to be entered for the TQ Core Component and/or relevant Occupational Specialist Component and/or an existing entry for a Student to be amended, the Supplier shall (where reasonably practicable having regard to the nature of the assessment) following receipt of a request from an Approved

Additional Service	Additional Service Requirements
	Provider within the period not greater than 20 Working Days prior to the commencement of the relevant assessment as determined in accordance with the relevant Key Dates Schedule, enter that Student for the TQ Core Component and/or relevant Occupational Specialist Component or amend that Student's entry for the TQ Core Component and/or relevant Occupational Specialist Component (as the case may be).
Very late registration or registration amendment	Where, following the very late registration deadline for the TQ specified in the Key Dates Schedule for the relevant Academic Year until the date on which registration for the TQ finally closes as specified in the Key Dates Schedule for the relevant Academic Year, an Approved Provider requires a new Student to be registered for the TQ and/or an existing registration for a Student to be amended, the Supplier shall (where reasonably practicable having regard to the nature of the assessment), following receipt of a request from an Approved Provider within the period not greater than 20 Working Days prior to the commencement of the relevant assessment as determined in accordance with the relevant Key Dates Schedule, register that Student for the TQ or amend that Student's registration for the TQ (as the case may be).

ANNEX 11 –

Schedule for the submission of; Supplementary Specimen Assessment Materials; Employer Set Project Guide Exemplar Responses; and Employer Set Project Grade Exemplar Responses

Product	Description	Authority Submission Date	Publication date	Review point
Core Component	Supplementary Specimen Assessment Materials covering the TQ Core Component in full (comprising the External Examination and the Employer Set Project)	By the end of August prior to the first Academic Year of teaching	By end of October during the first Academic Year	Commencing during the second Academic Year of teaching, to be reviewed by the Supplier each and every Academic Year and re-submitted to the Authority to agree any changes by the end of October, for re-publication by the end of December.
Occupational Specialist Component(s)	Supplementary Specimen Assessment Materials covering the Occupational Specialist Component(s) in full	By the end of March during the first Academic Year of teaching	By end of July during the first Academic Year	Commencing during the second Academic Year of teaching, to be reviewed by the Supplier each and every Academic Year and re-submitted to the Authority to agree any changes by the end of July, for re-publication by the end of October in the following Academic Year.
Employer Set Project Guide Exemplar Responses	Employer Set Project Guide Exemplar Responses covering the Employer Set Project, produced at grade A and grade E for each Employer Set Project, in consultation with Employers and accompanied by an explanatory commentary.	By the end of August prior to the first Academic Year of teaching	By end of October during the first Academic Year	
Employer Set Project Grade Exemplar Responses	Employer Set Project Grade Exemplar Responses covering the Employer Set Project, consisting of actual marked examples of Students' assessment evidence, selected after awarding, produced at grade A and grade E, for each Employer	By the end of October during the second Academic Year of teaching	By end of December during the second Academic Year	Commencing during the third Academic Year of teaching, to be reviewed by the Supplier each and every Academic Year and re-submitted to the Authority to agree any changes by the start of

	Set Project, in consultation with Employers and accompanied by an explanatory commentary.			September, for re-publication by the end of October.

* Where no students have sat an ESP, or no students have achieved a pass at grades A or E, on agreement with the Authority the Supplier may defer production of the Employer Set Project Grade Exemplar Responses to the next Academic Year.

Schedule 2 Annex 3

TQ Spec

S2_A3_GEN2W1_DSS_TQ_Spec

T-LEVELS | Institute for Apprenticeships & Technical Education

Qualification specification

T Level Technical Qualification in Digital Support Services

T Level Technical Qualification in Digital Support Services

Qualification Specification

Digital Support Services

603/6901/2

Contents

Section 1: Introduction 5

About this TQ specification 6

Section 2: Summaries 7

Technical qualification summary 7

Grading 9
Assessment method 9
Progression including job roles (where applicable) 10
UCAS 10
Regulation information 10
Funding 11
English, mathematics and digital content 11
Entry guidance 11
Transition programme 11
Registering students on T Levels 11
Transferring between T Levels and occupational specialisms (OSs) 12
Achieving this qualification 12
Retakes 12

Technical qualification components 14

Employer involvement 15
Progression to higher level studies 15
How the qualification is assessed 16
Assessment of English, maths and digital 16
Quality of written communication (QWC) 16
Application of mathematics, significant figures and decimal places 17
Digital skills 17
Rationale for synoptic assessment 17

Scheme of assessment for each component 17

External examinations (core component) 17

Overview of assessment 17
Employer set project (core component) 20
Synoptic assignments (Digital Infrastructure) 23
Synoptic assignments (Digital Support) 25
Assessment conditions 26
Synoptic assignments (Cyber Security) 26
Core written examinations 27
Sample assessment materials 28

Results 28
Enquiries about results 28

Grading....29

Core component 29
U grades 39
Awarding the final grade for each component of the TQ 39
Calculating the final grade for the T Level programme 39

Section 3: Frameworks....41

General competency framework....41

English, mathematics and digital competencies relevant to the Digital Support Service technical qualification....42

Section 4: TQ content....44

Qualification structure 44
Delivery of content 44

What you need to teach....44

Route core elements....45

Route core element 1: Business context 45
Route core element 2: Culture 56
Route core element 3: Data 57
Route core element 4: Digital analysis 64
Route core element 5: Digital environments 65
Route core element 6: Diversity and inclusion 71
Route core element 7: Learning 73
Route core element 8: Legislation 76
Route core element 9: Planning 80
Route core element 10: Security 82
Route core element 11: Testing 88
Route core element 12: Tools 90

The pathway core: Core knowledge and understanding across digital support services....93

Pathway core element 1: Careers within the digital support services sector 93
Pathway core element 2: Communication in digital support services 98
Pathway core element 3: Fault analysis and problem resolution 100

Core skills....102

Core skill 1: Communicate information clearly to technical and non-technical stakeholders 102
Core skill 2: Working with stakeholders to clarify and consider options to meet requirements 103
Core skill 3: Apply a logical approach to solving problems, identifying and resolving faults, whilst recording progress and solutions to meet requirements 104
Core skill 4: Ensure activity avoids risks to security 105

Occupational specialism: Digital Infrastructure....107

Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data 107
Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure 131
Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge 145

Occupational specialism: Network Cabling....150

Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data 150

Performance outcome 2: Install and test cabling in line with technical and security requirements 169
Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge 194
Occupational specialism: Digital Support....199
Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data 199
Performance outcome 2: Install, configure and support software applications and operating systems 219
Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge 240
Occupational specialism: Cyber Security....246
Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data 246
Performance outcome 2: Propose remediation advice for a security risk assessment 264
Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge 281
Section 5: TQ glossary....289
Section 6: Additional information....290
Annual monitoring visits 290
Guided learning hours (GLH) 290
Total qualification time (TQT) 290
Essential skills 290
Recognition of prior learning (RPL) 291
Qualification dates 291
Staffing requirements 291
Resource requirements 292
Customer support team 296
Fees and pricing 296
Training and support for providers 296
Useful websites and sources of information 297
Learning resources 297
Equal opportunities 297
Diversity, access and inclusion 297
Reasonable adjustments and special considerations policy 298
Contact us....299
Document information....300
Change history record 300

Section 1: Introduction

A T Level[1] is a composite technical study programme, aimed at preparing young people for work, higher level apprenticeships or higher education (HE). It comprises 5 key components:

- an approved technical qualification, which includes the opportunity to specialise in at least one occupational role
- a substantial industry placement with an external employer (further information regarding the required number of hours can be found on page 8)
- English, mathematics and digital requirements; students will have to achieve a minimum of level 2 English and mathematics in order to achieve a T Level (with some flexibility for students with special educational needs or disabilities (SEND))
- employability, enrichment and pastoral elements (EEP)
- in some cases, it may also include mandatory additional requirements (MAR), such as important licence to practise qualifications

The T Level Technical Qualification in Digital Support Services forms part of the new T Level in digital support services. The outline content has been produced by T Level panels based on the same standards as those used for apprenticeships. The outline content formed the basis of this qualification and has been further developed by NCFE.

This qualification has 2 components:

- core component:
  - route core
  - pathway core
- occupational specialism components:
  - Digital Infrastructure
  - Network Cabling
  - Digital Support
  - Cyber Security

The route core provides a variety of knowledge and skills relevant to the digital route as a whole. The pathway core provides a variety of knowledge and skills relevant to the occupational specialism components within the Digital Support Services TQ. Some of the pathway core topics and ideas are broken down and contextualised in more detail within the occupational specialisms, allowing students to apply the knowledge and skills in their own specific specialism.

[1] T Level is a registered trademark of the Institute for Apprenticeships and Technical Education

Each occupational specialism component covers the knowledge, understanding, skills and behaviours required to achieve threshold competence in a chosen occupational specialism. Threshold competence refers to the level of competence deemed by employers as sufficient to secure employment in roles relevant to an occupational specialism. Achievement of threshold competence signals that a student is well-placed to develop full occupational competence, with further support and development, once in work.

English, mathematics and digital skills have also been embedded throughout the technical qualification (TQ) and must be taught when highlighted in the content.

About this TQ specification

To ensure that you are using the most up-to-date version of this TQ specification, please check the version number and date in the page footer against that of the TQ specification on the NCFE website.

If you advertise this qualification using a different or shortened name, you must ensure that students are aware that their results will state the full regulated qualification title.

Section 2: Summaries

Technical qualification summary

Qualification title

T Level Technical Qualification in Digital Support Services

Qualification number (QN)

603/6901/2

Aim reference

60369012

Qualification level

3

Guided learning hours (GLH) and total qualification time (TQT)

Digital Infrastructure	GLH for delivery	GLH for assessment	Total GLH	TQT
Core component	584	16 hours 40 minutes	600 hours 40 minutes	647
Occupational specialism	575	24 hours 30 minutes	599 hours 30 minutes	657
Total			1200 hours 10 minutes	1304

Network Cabling	GLH for delivery	GLH for assessment	Total GLH	TQT
Core component	584	16 hours 40 minutes	600 hours 40 minutes	647
Occupational specialism	569	31	600	657
Total			1200 hours 40 minutes	1304

Digital Support	GLH for delivery	GLH for assessment	Total GLH	TQT
Core component	584	16 hours 40 minutes	600 hours 40 minutes	647
Occupational specialism	566	34	600	657

Total			1200 hours 40 minutes	1304

Cyber Security	**GLH for delivery**	**GLH for assessment**	**Total GLH**	**TQT**
Core component	584	16 hours 40 minutes	600 hours 40 minutes	661
Occupational specialism	569	27 hours 30 minutes	596 hours 30 minutes	657
Total			1197 hours 10 minutes	1318

The GLH only include time for the technical qualification element of the T Level programme; they do not include time allocated for the additional components of the T Level programme.

Minimum age

T Level Technical qualification students must be a minimum of 16 years of age.

Qualification purpose

The purpose of the T Level Technical Qualification in Digital Support Services is to ensure students have the knowledge and skills needed to progress into skilled employment or higher level technical training relevant to the T Level.

Objectives

The objectives of this qualification are to equip students with:

- the core knowledge and skills relevant to digital support services
- up-to-date occupational knowledge and skills that have continued currency amongst employers and others
- the necessary English, mathematics and digital skills
- threshold competence that meets employer expectations and is as close to full occupational competence as possible
- opportunities to manage and improve their own performance

Industry placement experience

Industry placements are intended to provide students with the opportunity to develop the knowledge, skills and behaviours required for skilled employment in their chosen occupation and which are less easily attainable by completing a qualification alone.

As part of achieving the overall T Level programme, students are required to complete a minimum of 315 hours industry placement. It is the provider's responsibility to ensure the minimum number of hours is undertaken by the student.

There may be specific requirements for providers and employers to consider prior to the student commencing a work placement. Please see the industry placement guidance from the Institute for Apprenticeships and Technical Education.

There are specific requirements for providers and employers relating to the insurance of students in the workplace. Further information about insurance can be found at www.abi.org.uk or www.hse.gov.uk/youngpeople/index.htm.

Rules of combination

Students are required to complete:

- core component:
  - route core
  - pathway core
- one occupational specialism component:
  - Digital Infrastructure
  - Network Cabling
  - Digital Support
  - Cyber Security

Students **must not** complete more than **one** occupational specialism component.

Approved providers can select which occupational specialism component to deliver to their students.

Grading

Component	Grade
Core component	A* to E and U
Occupational specialism component	Distinction/merit/pass and ungraded

Assessment method

Core component:

- 2 written examinations
- employer set project (ESP)

In order to achieve a grade for the core component, students must have results for both sub-components (the core (written) examination and the ESP).

The combined results from these sub-components will be aggregated to form the overall core component grade (A*–E and U).

If students fail to reach the minimum standard across all sub-components, they will receive a U grade. No overall grade will be issued for the core component until both sub-components have been attempted.

Occupational specialism component:

- synoptic assignments

The student is also required to successfully achieve a distinction/merit/pass grade in one of the occupational specialism components. If the student fails to reach the specified level of attainment, they will receive a U grade.

Progression including job roles (where applicable)

Students who achieve this qualification could progress to the following, depending on their chosen occupational specialism:

- employment:
  - digital support technician:
    - digital applications technician
    - digital service technician
  - infrastructure technician
  - IT solutions technician:
    - hardware solutions
    - software solutions
  - cyber security technician
  - network cable installer
- higher education
- apprenticeship (progression onto lower level apprenticeships may also be possible in some circumstances, if the content is sufficiently different)

UCAS

The T Level study programme is eligible for UCAS points. Please check the UCAS website for more information.

Regulation information

This is a regulated qualification. The regulated number for this qualification will be completed following Ofqual accreditation.

Funding

This qualification is eligible for funding. For further guidance on funding, please contact the Education and Skills Funding Agency (ESFA).

English, mathematics and digital content

English, mathematics and digital content are embedded and contextualised within the core skills and occupational specialism qualification content. This content must be taught to all students and will be subject to assessment.

Entry guidance

This qualification is designed for post-16 students.

There are no specific prior skills/knowledge a student must have for this qualification. However, students would be expected to have a level 2 qualification or equivalent.

Providers are responsible for ensuring that this qualification is appropriate for the age and ability of students. Providers must make sure that students can fulfil the requirements of the core component and chosen occupational specialism and comply with the relevant literacy, numeracy, digital and health and safety aspects of this qualification.

Students registered on this qualification should not undertake another qualification at the same level with the same or a similar title, as duplication of learning may affect funding eligibility.

Transition programme

For those students who are not yet ready to start a T Level programme at 16, they will be able to study a new T Level Transition Programme. This is a new 16 to 19 study programme designed to give young people effective, tailored preparation specifically to help them progress onto and succeed in a T Level.

The T Level Transition Programme will be introduced through phased implementation, working initially with a small number of volunteer T Level schools, colleges and training companies, to explore different approaches to delivery and develop good practice in effectively preparing students for a T Level. More information on the T Level Transition Programme can be found on the government’s website.

Registering students on T Levels

We expect students to make a decision about their T Level pathway within the first few weeks of their course, supported by good information, advice and guidance from their provider. For example, a student might know that they want to do a Digital T Level, but not be clear at the outset whether that should be Digital Production, Design and Development, Digital Support Services or Digital Business Services. If a provider is offering 2 or 3 of the available pathways, there may be some co-delivery or other activity in the first few weeks that provides students with the opportunity to find out about different occupations, for example through employer visits. A student’s chosen T Level pathway and occupational specialism (OS) should be recorded on the Individual Learner Record (ILR) or School Census in October of year 1.

To ensure there is sufficient time to cover the curriculum, decisions about OSs should be confirmed by the end of the first year, although this could be much earlier depending on a provider’s curriculum model. For example, some providers start teaching the OS early on in first year and require students to make a decision about this at the start

of their course, whereas other providers may only start teaching OSs in the second year. In order to ensure that providers receive the right level of funding, a student's OS must be confirmed in the final data return of year 1 (ILR R14/Autumn Census), although changes after this date are possible.

Providers will also need to ensure that they register their students on the TQ with the awarding organisation and enter them for assessments as relevant.

Transferring between T Levels and occupational specialisms (OSs)

We expect some students to switch between T Levels. Providers should consider the degree of overlap between the 2 T Levels and the remaining time before any assessments in determining if a transfer is possible, or whether a student will need to restart their T Level. Attainment from one T Level cannot count towards another, and all students will need to take and pass the relevant assessments in order to pass their T Level.

Some students may also want to switch to a different OS within the same T Level pathway, including in the second year. It is less likely that there will be any overlap between OSs, so any decision will depend on the provider's curriculum model and the stage a student has reached in their OS learning. Any changes to a student's T Level, whether pathway or OS, should be recorded on the ILR/Census as soon as possible and should also match the registration and assessment entries submitted to the relevant awarding organisation.

Achieving this qualification

To achieve this qualification, the student must successfully demonstrate their achievement of the core component and one occupational specialism component.

In order to achieve a grade for the core component, the student must attempt both the external examination (paper A and paper B) and ESP sub-components. The results from these will be aggregated to form the overall core component grade (A* to E and U). If students do not attempt one of the sub-components, an overall component grade will be withheld pending the attempt of both. If students fail to reach the minimum standard across sub-components after attempting both, they will receive a U grade for the component.

The student is required to successfully achieve a distinction/merit/pass grade in one of the occupational specialism components. If the student fails to reach the specified level of attainment, they will receive a U grade.

Retakes

Core component retakes

There is the opportunity for students to retake the core component assessments in order to improve their marks. This includes:

- 2 written examinations
- ESP

The core component's written examination is made up of 2 papers. If the student wants to retake the written examination assessment, they must retake **both** papers, in the same series.

Students can retake the core components in different series, meaning they could sit the ESP in one series and the core exams (both exam papers to be taken in the same series) in the next. There is no limit to the number of

retakes a student can complete. However, any retake must be completed within 2 years after the completion of the student's T Level programme.

When determining each student’s overall achievement for the core component, the highest achievement in each core component assessment (written examination and ESP) is used.

Occupational specialism component retakes

Although retakes are permitted for the occupational specialism, it is unlikely that students will be able to fit a retake opportunity into the delivery timetable.

If a retake opportunity is scheduled, the student must retake all synoptic assignments for the chosen occupational specialism. There will be one opportunity per year to sit the occupational specialism, meaning a retake of the occupational specialism would be sat in the next academic year of study.

There is no limit to the number of retakes a student can complete. However, any retake must be completed within 2 years after the completion of the student's T Level programme.

Technical qualification components

Component	Level	Content
Route core component	3	R1. Business context R2. Culture R3. Data R4. Digital analysis R5. Digital environments R6. Diversity and inclusion R7. Learning R8. Legislation R9. Planning R10. Security R11. Testing R12. Tools
Pathway core component	3	P1. Careers within the digital support services sector P2. Communication in digital support services P3. Fault analysis and problem resolution

Students are required to complete one occupational specialism component.

Component	Level	Content
Digital Infrastructure	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure • Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge
Network Cabling	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Install and test cabling in line with technical and security requirements

Component	Level	Content
		• Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge
Digital Support	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Install, configure and support software applications and operating systems • Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge
Cyber Security	3	• Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data • Performance outcome 2: Propose remediation advice for a security risk assessment • Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Employer involvement

The outline content for this qualification was devised by T Level panels. The panels consisted of employers and industry stakeholders.

We have worked in partnership with employers and other stakeholders to elaborate the content further, create the assessments and set the standards to ensure students achieve the level of competence needed to enter skilled employment.

Progression to higher level studies

This qualification aims to provide students with a number of progression options, including higher level studies at university or further education (FE) colleges. The skills required to progress to higher academic studies are different from those required at levels 1 and 2. Level 3 qualifications enable the development of these skills. Although there is no single definition of higher level learning skills, they include:

- checking and testing information
- supporting points with evidence
- self-directed study
- self-motivation
- thinking for yourself
- analysing and synthesising information/materials
- critical thinking and problem solving

- working collaboratively
- reflecting upon learning and identifying improvements
- presenting information in written and verbal formats

Level 3 criteria can require students to analyse, draw conclusions, interpret or justify, which are all examples of higher level skills and support progression and further learning. If you need any further information, please refer to the NCFE website.

How the qualification is assessed

Assessment is the process of measuring a student's skill, knowledge and understanding against the standards set in a qualification.

The core component (route core and pathway core) is 100% externally assessed. External assessments are set and marked by NCFE. The external examinations and ESP will assess students' core knowledge, understanding and skills relevant to the occupations within the Digital Support Services TQ. Students may be entered for any assessment window of the core component assessments that is most appropriate for them, although, in the case of the core external examinations, they must take the 2 examinations in the same sitting.

The occupational specialism components are also externally assessed through synoptic assignments. These synoptic assignments will assess the knowledge, understanding, skills and behaviours required to achieve threshold competence in the student's chosen occupational specialism.

Providers must not give any feedback to the student about their performance in any of the externally assessed components or elements.

The assessment consists of:

- core component:
  - 2 written examinations
  - ESP
- occupational specialism component:
  - synoptic assignments (specific to each occupational specialism)

Assessment of English, maths and digital

The TQ outline content has been reviewed against the general competency frameworks for English, mathematics and digital (EMD). The resulting mapping document is contained in section 3.

For the purposes of the core tests, English skills will be assessed through the students' ability to convey ideas precisely and accurately and be referred to as quality of written communication (QWC).

Quality of written communication (QWC)

Quality of written communication is assessed within targeted marks for the core examinations and are embedded throughout the assessment objectives within the ESP. No specific marks are available within the occupational specialism; however, a good command of communication and written work is anticipated for success at this level.

Application of mathematics, significant figures and decimal places

Throughout the core component examinations for all pathways, students will be assessed on their understanding and application of mathematics. Some questions may require answers to be given to a number of significant figures or a given number of decimal places.

A paper may contain marks that are dependent on students giving final answers to a specified number of significant figures or decimal places. A significant figure mark may not be awarded for an answer given in surd form. In questions where the command word is 'calculate' and the final answer is required in either format, the question should be calculated to at least one additional significant figure or decimal place before giving the final answer as requested in the question.

In all cases where an answer is required to a number of significant figures or decimal places, this will be specified in the question.

Digital skills

Digital skills are expected to be naturally occurring in the ESP and occupational specialism; marks are allocated where they are deemed to occur naturally in the completion of the task.

Rationale for synoptic assessment

Synoptic assessments test students' understanding of the connections between the topics covered across the performance outcomes within the chosen occupational specialism.

Synoptic assessment enables students to integrate and apply knowledge, understanding and skills with breadth and depth. It also requires them to demonstrate their capability to apply knowledge, understanding and skills across the chosen occupational specialism.

Scheme of assessment for each component

Each component in the core is worth the following weighting:

	% weighting of the core component
Paper A	34
Paper B	41
Sub-total	75
ESP	25
Total	**100%**

External examinations (core component)

Overview of assessment

Paper A
Written examination

Duration: 2 hours

100 Marks (plus 6 marks for quality of written communication) = 106 marks total

This paper covers 50% of the core knowledge and understanding.

This paper is composed of 3 sections, which may consist of multiple choice questions, short-answer and extended writing:

- Section A: Business context (element 1) and Culture (element 2): 38–44 marks
- Section B: Diversity and inclusion (element 6) and Digital environments (element 5): 36–42 marks
- Section C: Learning (element 7) and Planning (element 9): 20–26 marks

Paper B
Written examination

Duration: 2 hours 30 minutes

125 Marks (plus 6 marks for quality of written communication) = 131 marks total

This paper covers 50% of the core knowledge and understanding.

This paper is composed of 4 sections which may consist of multiple choice questions, short-answer and extended writing:

- Section A: Digital Support Services pathway: 25 marks
- Section B: Tools (element 12) and Testing (element 11): 18–24 marks
- Section C: Security (element 10) and Legislation (element 8): 34–40 marks
- Section D: Data (element 3) and Digital analysis (element 4): 40–46 marks

Content subject to assessment

- Paper A:
  - route core elements: 1, 2, 5, 6, 7 and 9
- Paper B:
  - route core elements: 3, 4, 8, 10, 11 and 12
  - pathway core element: 1, 2 and 3

Assessment objectives and weightings

The external (core component) examinations will assess how students have achieved the following assessment objectives (AOs).

	Assessment objectives	Weighting*
AO1	Demonstrate knowledge and understanding of the digital support services sector	28%
AO2	Apply knowledge and understanding of the digital support services sector to different situations and contexts	40%
AO3	Analyse and evaluate information and issues related to the digital support services sector	32%

*Both paper A and paper B allocate 6 marks to the Quality of Written Communication (QWC). These marks are bolted on and do not impact on the AO weightings. For example, paper A totals 106 marks of which the AO weightings apply to a total of 100 marks, with the remaining 6 assessing QWC.

Total marks

AOs	Paper A	Paper B	Total
AO1	28 marks (14%)	35 marks (14%)	63 marks (28%)
AO2	40 marks (20%)	50 marks (20%)	90 marks (40%)
AO3	32 marks (16%)	40 marks (16%)	72 marks (32%)
QWC	6 marks	6 marks	12 marks
Total	**106 marks**	**131 marks**	**237 marks**

The table above shows how the core examination will target the AOs in this qualification. Each version of the core examination will adhere to these mark and percentage weighting. Both paper A and paper B allocate 6 marks to the Quality of Written Communication (QWC). These marks are bolted on and do not impact on the AO weightings.

Assessment availability

There will be 2 assessment opportunities per year in Summer (May/June) and Autumn (November/December). Please refer to the Assessment timetable on the NCFE website for further information.

Assessment conditions

The core component external examinations must be invigilated.

All students' scripts must be submitted to NCFE for marking. All assessment material must be securely stored by the approved provider. On-screen assessments will be submitted through the online assessment platform.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Employer set project (core component)

Overview of assessment

Externally set (in conjunction with employers) project

The purpose of the employer set project is to ensure that students have the opportunity to apply core knowledge and skills to develop a substantial piece of work in response to an employer set brief. The brief and tasks are contextualised around an occupational area and chosen by the student ahead of the assessment window.

To achieve the AOs and meet the brief, the student must demonstrate the following core skills:

Core skill 1	Communicate information clearly to a technical and non-technical audience
Core skill 2	Work with stakeholders to clarify and consider options to meet requirements
Core skill 3	Apply a logical approach to solving problems, identifying and resolving faults whilst recording progress and solutions
Core skill 4	Ensure activity avoids risks to security

The knowledge requirements will be taken from the core knowledge relevant to the brief; the briefs will change for each assessment window.

Duration: 12 hours 10 minutes

Subject content to be assessed

Content subject to assessment – route core elements: 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12:

- core skills assessment objectives and core knowledge

Pathway core elements: 1, 2, 3

Core knowledge relevant to the brief will be covered in the employer set project; this will change for each assessment window.

Core skills

In completing the employer set project, the student will demonstrate 4 core skills, supported by underpinning knowledge and understanding set out in the core content.

Core skill 1	Communicate information clearly to a technical and non-technical audience
Core skill 2	Work with stakeholders to clarify and consider options to meet requirements

Core skill 3	Apply a logical approach to solving problems, identifying and resolving faults whilst recording progress and solutions
Core skill 4	Ensure activity avoids risks to security

Assessment objective (AO)		**AO weighting**
AO1	Plan their approach to meeting the project brief	16 marks (21)%
AO2	Apply core knowledge and skills as appropriate to infrastructure support and maintenance	40 marks (52.5)%
AO3	Select relevant techniques and resources to meet the brief	6 marks (8)%
AO4	Use English, mathematics and digital skills as appropriate	6 marks (8)%
AO5	Realise a project outcome and review how well the outcome meets the brief	8 marks (10.5)%

Task	**AO1**	**AO2**	**AO3**	**AO4 (Maths)**	**AO4 (English)**	**AO5**	**TOTAL**
1		16	6				22
2	8	4			4*		12*
3	8	16		2			26*
4		4				8	12*
Total marks	16	40	6	6		8	76* (when the x4 AO4 English are included)

*AO4 (English) is assessed holistically across tasks 2, 3 and 4 using two level of response mark schemes and is not included in the individual task totals - only the overall ESP total.

Assessment availability

There will be 2 assessment opportunities per year in Summer (May/June) and Autumn (November/December). Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under supervised conditions. This means students can access resources in order to complete their assessment.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

UMS

The core component is modular, which means that a student can take and resit the assessments in different assessment windows. Assessments may vary slightly in levels of difficulty and, therefore, the mark that represented a C grade in the external examination in one assessment window may not be appropriate in the following assessment window.

To address this, we convert raw marks to uniform marks. The UMS also allows us to account for the relative weighting of the assessment to the qualification as a whole. The maximum UMS points available for each assessment, and the UMS points relating to each grade boundary, are fixed. These are shown in the following table:

Grade boundary	External examination	Employer set project	Overall
Max	300	100	400
A*	270	90	360
A	240	80	320
B	210	70	280
C	180	60	240
D	150	50	200
E	120	40	160
U	0	0	0

The external examination comprises 2 papers, the results of which are combined before conversion to UMS. Combined grade boundaries for each series will be set by adding together the equivalent boundaries for each paper.

The raw mark grade boundaries are set after each assessment window. NCFE sets these boundaries judgementally, following both qualitative and quantitative analysis, and then converts them to UMS.

Although the raw mark grade boundaries in assessment window 1 and assessment window 2 are different, they have the same value in terms of UMS marks (for example 180 for a C and 210 for a B) when contributing to the qualification as a whole. NCFE will publish the raw mark grade boundaries following the completion of each assessment window.

Synoptic assignments (Digital Infrastructure)

Synoptic assignments comprise task-based assignments.

Duration: 24 hours 30 minutes

Consisting of:

- assignment 1: 13 hours
- assignment 2: 6 hours
- assignment 3: 5 hours 30 minutes

Content subject to assessment

All performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	35%	76	1.000	76.000
Assignment 2	35%	53	1.434	76.000
Assignment 3	30%	56	1.163	65.143
Total	100%	185 marks		*217*

Total marks 185

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from Summer 2023. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Synoptic assignments (Network Cabling)

Synoptic assignments comprise task-based assignments.

Duration: 31 hours

Consisting of:

- assignment 1: 13 hours
- assignment 2: 12 hours 30 minutes
- assignment 3: 5 hours 30 minutes

Content subject to assessment

All performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install and test cabling in line with technical and security requirements
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	30%	60	1.017	61.000
Assignment 2	40%	44	1.848	81.333
Assignment 3	30%	61	1.000	61.000
Total	100%	165 marks		*203*

Total marks 165

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from Summer 2023. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Synoptic assignments (Digital Support)

Synoptic assignments comprise task-based assignments.

Duration: 34 hours

Consisting of:

- assignment 1: 19 hours
- assignment 2: 5 hours
- assignment 3: 10 hours

Content subject to assessment

All performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install, configure and support software applications and operating systems
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	50%	76	1.000	76.000

Assignment 2	20%	30	1.013	30.400
Assignment 3	30%	27	1.689	45.600
Total	100%	133 marks		*152*

Total marks 133

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from Summer 2023. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Synoptic assignments (Cyber Security)

Synoptic assignments comprise task-based assignments.

Duration: 27 hours 30 minutes

Consisting of:

- assignment 1: 11 hours
- assignment 2: 10 hours 30 minutes
- assignment 3: 6 hours

Content subject to assessment

All Performance outcomes within a chosen occupational specialism are subject to assessment:

- Performance outcome1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome2: Propose remediation advice for a security risk assessment
- Performance outcome3: Discover, evaluate and apply reliable sources of knowledge

Assessment weightings

Assignment	% weighting of the Occupational Specialism	Max raw mark	Scaling factor*	Maximum scaled mark
Assignment 1	20%	50	1.000	50.000
Assignment 2	40%	60	1.667	100.000
Assignment 3	40%	70	1.429	100.000
Total	100%	180 marks		250

Total marks 180

*Scaled marks for assignments are calculated by multiplying the raw assessment mark with the scaling factor. Scaled marks up to 3 decimal places are combined before being rounded to the nearest whole number. The same approach is used to determine overall combined grade boundaries from assignment grade boundaries.

Assessment availability

There will be one assessment opportunity per year from summer 2025. Please refer to the assessment timetable on the NCFE website for further information.

Assessment conditions

All tasks must be completed under specified conditions. See the tutor guidance in the tutor guidance pack for more detail.

The approved provider must securely retain all students' evidence and submit that evidence to NCFE for marking.

Please refer to the regulation for the conduct of external assessments for further information on the assessment conditions. Please refer to the NCFE website for an up-to-date copy of the regulations.

Core written examinations

The core written examinations will be available as onscreen and as paper-based examinations. A different version of each examination will be available per mode.

The ESP and the occupational specialism assessments will be released and accessed by providers electronically. The submission of any assessment evidence from providers will also be digital and provided to NCFE electronically, unless otherwise specified.

For instructions on conducting external assessments (including information on malpractice/maladministration), please refer to our regulation for the conduct of external assessments and qualification specific instructions for delivery documents, which are available on the Policies & Documents page on the NCFE website.

Sample assessment materials

Sample assessment materials can be found on the qualification page on the NCFE website.

Results

Results for each component will be released in accordance with the assessment windows. Please refer to the assessment windows on the NCFE website for further information.

Enquiries about results

If a provider believes a student's result is at variance with their reasonable expectations, they can submit an enquiry about a result in line with our enquiries about results and assessment decisions policy, which is available on the Policies & Documents page on the NCFE website.

Grading

Core component

The core component is graded A* to E and U.

Core component grade descriptors

Grade	Demonstration of attainment
A	A grade A student can:
	use technical terminology accurately and consistently in a relevant and appropriate way
	demonstrate a comprehensive understanding of ideas, processes and procedures applied to familiar and unfamiliar contexts
	accurately use a range of mathematical skills relevant to the sector to support their application of key concepts, for example: • confidently convert from binary to decimal and vice versa • recognises hexadecimal and settings where it may be applied • applies concepts, such as ‘kilo, mega, tera’ • recognises the difference between bits and bytes
	critically analyse most information and data, supported with relevant examples and analysis: • will access a wide range of tools to gather data • is able to configure tools effectively to support their data analysis
	construct a reasoned argument, make substantiated judgements and reach valid conclusions
	effectively organise and present information clearly, supported with relevant examples and analysis
	comment effectively on strengths and limitations
	link together appropriate principles and concepts from the sector
E	A grade E student can:
	use technical terminology on occasion and may show some relevance at times

Grade	Demonstration of attainment
	demonstrate basic understanding of ideas, processes and procedures, applied to some familiar and unfamiliar contexts
	use some simple mathematical skills relevant to the sector to help support basic understanding of key concepts, for example: • struggles when converting from binary to decimal and vice versa • is aware of hexadecimal and is limited in recognising where this is applied • applies concepts such as 'kilo, mega, tera' with limited accuracy • is aware of a difference between bits and bytes but may confuse the application of these terms
	provide limited analysis of information, ideas and research: • accesses a limited range of simple tools to gather data • is limited in their configuration of tools to support their data analysis
	organise and present information, supported with rudimentary examples and some acceptable analysis
	comment on strengths and limitations
	put together some principles and concepts from the sector

Occupational specialism components

The occupational specialism components are graded distinction, merit, pass and ungraded.

Digital Infrastructure occupational specialism grade descriptors

Grade	Demonstration of attainment
Pass	The evidence showing installations and configuration setup is logical and displays sufficient knowledge in response to the demands of the brief.
	The student makes some use of relevant knowledge and understanding of implementing network infrastructure but demonstrates adequate understanding of perspectives or approaches associated with industry standards in digital infrastructure roles.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their implementations and configurations.

	The student is able to identify some information from appropriate sources and apply the appropriate information/appraise relevancy of information and can combine information to make some decisions.
	The student makes sufficient judgements/takes appropriate action/seeks clarification with guidance and is able to make adequate progress towards prioritising and solving non-routine problems in real life situations.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques to plan, install, configure, deploy and populate network infrastructure and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to attempt to prioritise and solve problems with some attempt at verifying their implementations.

Grade	Demonstration of attainment
Distinction	The evidence is precise and logical, showing installations, configuration and deployment that provides a detailed and informative response to the demands of the brief.
	The student makes extensive use of relevant knowledge and has extensive understanding of the practices of the sector and demonstrates a depth of understanding of the different perspectives/approaches associated with installing, testing, monitoring and maintaining digital infrastructure.
	The student makes decisive use of facts/theories/approaches/concepts, demonstrating extensive breadth and depth of knowledge and understanding and selects highly appropriate skills/techniques/methods to apply network infrastructure practices.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can combine information to make coherent decisions.
	The student makes well-founded judgements/takes appropriate action/seeks clarification and guidance and is able to use that to reflect on real life situations in a digital infrastructure role; being able to apply implementation and configuration of the network.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in a digital infrastructure role and precisely applies this across a variety of contexts and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.
	The student can thoroughly examine data/information in context and apply appropriate analysis in confirming or refuting conclusions and carrying out further work to justify and evaluate strategies for solving problems, giving concise explanations for their reasoning.

Network Cabling occupational specialism grade descriptors

Grade	Demonstration of attainment
Pass	The network diagrams are logical and display sufficient knowledge in response to the demands of the brief.
	The student makes some use of relevant knowledge and understanding of network cabling theories and practices but demonstrates adequate understanding of perspectives or approaches associated with industry best practice.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their designs and implementation, as well as in their testing and documentation.
	The student is able to identify some information from appropriate sources and makes use of appropriate information/appraise relevancy of information and can combine information to support decision making.
	The student makes sufficient judgements/takes some appropriate action/seeks clarification with guidance and is able to make adequate progress towards solving faults with network cables or resolving faults found in testing.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques reflected in network cabling, design and implementation and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to find solutions to problems and make some justification for strategies for solving problems.

Grade	Demonstration of attainment
Distinction	The network designed and developed is precise, logical and provides a detailed and informative resolution to the demands of the brief.
	The student makes extensive use of relevant knowledge, has extensive understanding of the network cabling practices and demonstrates an understanding of the different perspectives/approaches associated with designing, installing and testing networks.
	The student makes decisive use of facts/theories/approaches/concepts in their designs, demonstrating extensive breadth and depth of knowledge, and understands and selects highly appropriate skills/techniques/methods to build and test their networks.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can combine information to make coherent decisions.
	The student makes well-founded judgements/takes appropriate action/seeks clarification and guidance and is able to use that to reflect on real life situations in resolving network cabling faults and network configuration.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in network cabling, design and implementation, and precisely applies this across a variety of contexts, and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.
	The student can thoroughly examine network requirements in context and apply appropriate analysis in confirming or refuting conclusions and carrying out further work to justify strategies for solving problems, giving concise explanations for their reasoning.

Digital Support occupational specialism grade descriptors

Grade	Demonstration of attainment
Pass	The evidence showing installations and setup is logical and displays sufficient knowledge in response to the demands of the brief.
	The student makes some use of relevant knowledge and understanding of setting up systems and demonstrates adequate understanding of perspectives or approaches associated with industry standards in digital support services roles.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their configurations.
	The student is able to identify some information from appropriate sources and apply the appropriate information/appraise relevancy of information and can combine information to make decisions.
	The student makes sufficient judgements/takes appropriate action/seeks clarification with guidance and is able to make adequate progress towards prioritising and solving non-routine problems in real life situations.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques to plan, install, configure and test software systems and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to attempt to prioritise and solve problems with some attempt at reasoning.

Grade	Demonstration of attainment
Distinction	The evidence is precise, logical and provides a detailed and informative response to the demands of the brief.
	The student makes extensive use of relevant knowledge, has extensive understanding of the practices of the sector and demonstrates a depth of understanding of the different perspectives/approaches associated with digital support.
	The student makes decisive use of facts/theories/approaches/concepts, demonstrating extensive breadth and depth of knowledge and understanding and selects highly appropriate skills/techniques/methods.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can combine information to make coherent decisions.
	The student makes well-founded judgements/takes appropriate action/seeks clarification and guidance and is able to use that to reflect on real life situations in a digital support role.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in a digital support role and precisely applies this across a variety of contexts, and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.
	The student can thoroughly examine data/information in context and apply appropriate analysis in confirming or refuting conclusions, carrying out further work to justify strategies for solving problems, giving concise explanations for their reasoning.

Cyber Security occupational specialism grade descriptors

Grade	Demonstration of attainment
Pass	The student is able to develop a project proposal to research and compare the current software available and justify their recommendations.
	The student is able to install supplied software onto a device and ensure it is all correctly configured.
	The student is able to identify and explain the difference between cyber attacks and software issues, and how a cyber attack could take place.
	The student is able to investigate the issues on the virtual machine provided and explain the most effective remedial action to take to mitigate any problems.
	The student is able to evaluate a network with regards to cyber security.
	The student is able to ensure that company resources and data are fully protected.
	The student is able to perform a security risk assessment of the site and the network.
	The student is able to recommend physical, administrative, and technical controls.
	The student is able to create a disaster recovery plan including recommendations in the case of service outages.
	The student is able to explain how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.

Grade	Demonstration of attainment
Distinction	The student is able to develop an in-depth project proposal to research and compare the current software available and comprehensively justify their recommendations.
	The student is able to install supplied software onto a device, demonstrating excellent capabilities in ensuring it is all correctly configured.
	The student is able to comprehensively identify and explain the difference between cyber attacks and software issues, and evidence a detailed understanding of how a cyber attack could take place.
	The student is able to thoroughly investigate the issues present on the virtual machine provided and fully justify the most effective remedial action to take to mitigate any problems.
	The student is able to carry out an in-depth evaluation of a network with regard to cyber security and identify areas of improvement.
	The student is able to perform an in-depth security risk assessment of the site and the network, identify areas of concern and give a rationale for each.
	The student is able to recommend physical, administrative, and technical controls and justify their recommendations.
	The student is able to create an in-depth disaster recovery plan, including justifications for recommendations in the case of service outages.
	The student is able to demonstrate in-depth knowledge and give a thorough explanation of how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.

“Threshold competence” refers to a level of competence that:

- signifies that a student is well-placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the TQ in a classroom-based setting (for example, in the classroom, workshops, simulated working and (where appropriate) supervised working environments)
- signifies that a student has achieved the level for a pass in relation to the relevant occupational specialism component

U grades

If a student is not successful in reaching the minimum threshold for the core and/or occupational specialism component, they will be issued with a U grade.

Awarding the final grade for each component of the TQ

Each core component’s marks will be combined to form the overall grade for the core component.

The marks from the occupational specialism assignment will form the occupational specialism grade.

These grades will be submitted to the Institute for Apprenticeships and Technical Education who will issue an overall grade for the T Level study programme.

Calculating the final grade for the T Level programme

To be awarded an overall T Level grade, a student must successfully pass both components of their TQ, complete an industry placement, achieve level 2 English and mathematics if they have not already achieved this prior to starting a T Level, and meet any other requirements set by the Institute’s T Level panel. T Levels will vary in size, largely dependent on the size of the TQ, and on whether a student needs to continue to study English and mathematics.

The full list of Functional Skills/GCSE/other alternative qualifications which meet the English and mathematics requirement for T Levels, including details of flexibility for students with SEND, is published in the Specification of apprenticeship standards for England (SASE), which is available via the Department for Education’s (DfE) website.

The overall grade for the T Level programme is based on a student’s performance in the TQ and would reflect:

- the comparative size of the core component and the occupational specialism
- the grades achieved for the core component (A* to E) and the occupational specialism (P/M/D)

This grading approach also makes it possible to recognise exceptional achievement, through the award of an overall distinction* grade for students that achieve an A* for the core component and a distinction in their occupational specialism.

The following table shows how the core component and occupational specialism grades are aggregated to produce an overall result for this T Level programme:

Core component 50% occupational specialism 50%:

Core component grade	Occupational specialism grade: Distinction	Merit	Pass
A*	distinction*	distinction	distinction
A	distinction	distinction	merit
B	distinction	merit	merit
C	distinction	merit	pass
D	merit	merit	pass
E	merit	pass	pass

Overall T Level grade

This matrix shows the overall TQ grade when both TQ components are combined. For example, if a student achieved a B grade in the core component assessment (indicated by the vertical column on the left) and a merit grade in the occupational specialism assessment (indicated by the horizontal top row), they would achieve a merit grade for the overall T Level programme:

Core component grade	Occupational specialism grade: Distinction	Merit	Pass
A*	distinction*	distinction	distinction
A	distinction	distinction	merit
B	distinction	merit	merit
C	distinction	merit	pass
D	merit	merit	pass
E	merit	pass	pass

merit

Section 3: Frameworks

General competency framework

Technical qualifications are required to contain sufficient and appropriate English, mathematical and digital content to help students reach threshold competence in their chosen specialism. As such, a framework of competencies has been developed which awarding organisations are required to use and embed in all technical qualifications (where appropriate).

General English competencies	General mathematical competencies	General digital competencies
GEC1. Convey technical information to different audiences	GMC1. Measuring with precision	GDC1. Use digital technology and media effectively
GEC2. Present information and ideas	GMC2. Estimating, calculating and error spotting	GDC2. Design, create and edit documents and digital media
GEC3. Create texts for different purposes and audiences	GMC3. Working with proportion	GDC3. Communicate and collaborate
GEC4. Summarise information/ideas	GMC4. Using rules and formulae	GDC4. Process and analyse numerical data
GEC5. Synthesise information	GMC5. Processing data	GDC5. Be safe and responsible online
GEC6. Take part in/lead discussions	GMC6. Understanding data and risk	GDC6. Controlling digital functions
	GMC7. Interpreting and representing with mathematical diagrams	
	GMC8. Communicating using mathematics	
	GMC9. Costing a project	
	GMC10. Optimising work processes	

The following table identifies the English, mathematical and digital competencies that we have embedded in skills throughout this technical qualification. The tutor may also teach competencies that are not listed here, where they naturally occur, but these will not be subject to assessment.

English, mathematics and digital competencies relevant to the Digital Support Service technical qualification

General competencies	Core skills	Digital Infrastructure	Network Cabling	Digital Support	Cyber Security
English					
GEC1	CS1, CS2, CS3	S2.1, S2.2, S2.6, S3.4, S3.5	S2.1, S2.7, S2.9, S2.10, S3.4, S3.5	S2.2, S2.6, S2.7, S3.4, S3.5	S2.4, S3.6
GEC2	CS1, CS2	S2.6	S2.1		S2.4
GEC3	CS1, CS2, CS3, CS4	S2.2, S3.4, S3.5, S3.6	S2.1, S2.6, S2.7, S2.9, S2.10, S3.5, S3.6	S2.6, S3.5, S3.6	S1.4, S2.3, S3.6
GEC4	CS1, CS4	S1.4, S1.5, S1.6, S2.1, S2.2, S2.6, S3.1, S.3.2, S3.3	S1.4, S1.5, S2.7, S2.9, S2.10, S3.1, S.3.2, S3.3	S1.4, S1.5, S1.6, S1.7, S2.2, S2.6, S2.7, S3.1, S.3.2, S3.3	S1.4, S2.3, S2.4, S3.6
GEC5		S1.1, S1.3, S2.2, S3.4, S3.5	S1.1, S1.3, S2.7, S3.4, S3.5	S1.1, S1.3, S3.4, S3.5	
GEC6	CS1, CS2			S2.7	S2.4, S3.6
Mathematics					
GMC1		S2.5	S2.1, S2.7		S2.1, S3.6
GMC2	CS2	S2.2, S2.5, S2.7	S2.1	S2.2	S2.1, S3.6
GMC3		S2.7		S2.2	S2.1, S3.5, S3.6
GMC4			S2.6		
GMC5	CS2, CS3	S1.6, S3.4, S3.6	S1.4, S2.1, S2.6, S3.4, S3.6	S1.6, S2.2, S2.7, S3.4, S3.6	S1.4, S2.2, S2.3, S3.1, S3.2, S3.3, S3.5
GMC6	CS4	S1.5, S2.2, S3.5, S3.6	S1.5, S3.5, S3.6	S1.5, S2.3, S2.7	S1.4, S2.1, S3.2, S3.4, S3.5

General competencies	Core skills	Digital Infrastructure	Network Cabling	Digital Support	Cyber Security
GMC7			S2.1, S2.5		
GMC8		S3.6	S2.7, S3.6	S3.6	S1.4, S2.1, S3.6
GMC9					
GMC10	CS1, CS2, CS3, CS4	S2.2	S2.9, S2.10	S1.7, S2.6	S1.5, S2.4, S3.6
Digital					
GDC1	CS1, CS2, CS3, CS4	S1.1, S1.4, S2.3, S2.4, S3.1	S1.1, S3.1	S1.1, S1.4, S1.7, S2.1, S2.2, S3.1	S1.3, S2.2, S3.3
GDC2	CS1	S3.3	S3.3	S3.3	
GDC3	CS1	S1.2, S3.4, S3.5, S3.6	S1.2, S2.1, S3.4, S3.5, S3.6	S1.2, S2.2, S2.4, S2.7, S3.4, S3.5, S3.6	S1.5, S2.4, S3.1, S3.5
GDC4	CS1, CS3, CS4	S1.5, S1.6, S2.6, 3.6	S1.4, S1.5, S2.7, S3.6	S1.5, S1.6, S2.4, S2.6, S2.7, S3.6	S1.6, S2.1, S2.3, S3.6
GDC5	CS1, CS2, CS4	S1.1, S1.3, S2.2, S3.2	S1.1, S1.3, S3.2	S1.1, S1.3, S1.7, S2.4, S3.2	S1.3, S2.2, S3.1, S3.2, S3.4, S3.5
GDC6	CS2	S1.1, S1.4, S2.3, S2.4	S1.1, S2.2, S2.4	S1.1, S1.4, S1.7, S2.1, S2.2, S2.5	S1.3, S2.4, S3.3

Section 4: TQ content

This section provides details of the structure and content of this qualification.

Qualification structure

The technical qualification (TQ) in Digital Support services has 2 components:

- core component, comprising route core, pathway core and core skills
- occupational specialism components:
    - Digital Infrastructure
    - Network Cabling
    - Digital Support
    - Cyber Security

The core content is divided into 12 route core elements, 3 pathway core elements and 4 core skills, all of which indicate the relevant knowledge and understanding of concepts, theories and principles relevant to all occupations within digital support services. The knowledge and skills are all externally assessed through written examinations and an ESP.

The occupational specialisms are divided into performance outcomes, each of which indicates the knowledge and skills required to enable students to achieve threshold competence in the chosen occupational specialism. These performance outcomes are all externally assessed through synoptic assignments, in which the student will be expected to demonstrate required knowledge and skills.

Delivery of content

The content does not have to be taught in a linear fashion. However, providers must pay attention to when the assessments are due to take place to ensure that all of the mandatory content (all elements and performance outcomes) has been taught to their students prior to sitting the assessments.

What you need to teach

This section contains all of the mandatory teaching content that underpins the knowledge and skills. The content provided in some cases may not be exhaustive, and providers may wish to teach beyond what is included in the specification to support the student's knowledge and understanding.

English, mathematics and digital competencies have been integrated and contextualised within the skills, throughout the qualification content. These competencies are mandatory and subject to assessment and must be delivered alongside the subject-specific content. The tutor may also teach competencies that are not listed in this specification, but these will not be subject to assessment.

Route core elements

Route core element 1: Business context

What you need to teach

The student must understand:

R1.1 Types of organisations and stakeholders within the business environment.

Organisation types:

- public
- private:
  - small or medium-sized enterprise (SME)
  - large enterprise
  - non-governmental organisation (NGOs)
- voluntary/charity:
  - not for profit

Stakeholder types:

- internal:
  - end users:
    - owners
    - board of directors
    - employees
    - departments
- external:
  - customers/consumers - purchases goods and services
  - clients - engages professional services
  - direct/indirect competitors
  - outsources services and suppliers
  - shareholders
  - investors
  - funders
  - government:
    - local

What you need to teach

- national
- international

Business environments:

- business to consumer (B2C)
- business to business (B2B)
- business to many (B2M)

R1.2 Key factors that can influence the business environment:

- political factors (for example cross party focus and agendas)
- economic factors (for example interest rates, consumer trends, periods of recession)
- social factors (for example social mobility, market trends, cultural expectations, socioeconomic aspects)
- technological factors (for example emerging technologies)
- legal factors (for example legislation changes and updates)
- environmental factors (for example carbon footprints, digital waste)

R1.3 The measurable value of digitalisation to a business:

- sales and marketing:
  - enhanced market research
  - increased opportunities for brand promotion
  - increased communication and coverage via social media
  - online opportunities for selling/e-commerce
  - tracking and management of customer/service-user retention
  - digital analytics (for example customer satisfaction scores)
- operations:
  - enhanced communication channels
  - automation of internal systems
  - remote working functionality
- finance:
  - increased fiscal performance
  - increased reporting options and functionality
  - reduced operating costs

What you need to teach

- key performance indicators (KPIs):
  - easier to monitor

R1.4 The influence and impact of digitalisation within a business context and market environment:

- brand differentiation:
  - brand values
- virtualisation/cloud solutions:
  - enabling scalable, elastic computing solutions to meet business demand
- digital innovations:
  - business intelligence and insight
  - unique selling points (USP)
- processes and business models:
  - digital manufacturing
  - financial
  - research
- wider access to:
  - customer base
  - range of product and services
- contextualising customer behaviour:
  - digital personalisation
  - platform interoperability
- open standards:
  - using non-platform specific digital identity

R1.5 The role of technical change management in digital operational integrity:

- preparation and planning:
  - innovations within digital technology
  - effectively communicating the rationale for the change
  - communicating the benefits of the change
  - getting ‘buy in’ from all areas of the business who the change effects
- operations:
  - interaction of new or upgraded tools and processes into current digital ecosystem

What you need to teach

- establishing best practice for use of new or upgraded tools and processes
- facilitating processes and business models
- applying fixes

R1.6 The components of technical change management:

- change advisory board (CAB):
  - prioritise change requests
  - review change requests
  - monitor change process
  - provide feedback
- request for change:
  - viability:
    - financial
    - resource
  - analysis of benefits of implementing change request
  - stages of approval
- setting SMARTER objectives:
  - specific
  - measurable
  - achievable
  - realistic
  - time-bound
  - evaluate
  - re-evaluate
- risks:
  - resistance to change from staff/teams
  - misuse of the new tools and processes
  - inadequate support, infrastructure or resource
  - change stalling or impeding workflows
  - knowledge management and single sources of dependencies
- impact:

What you need to teach

- forecasting the impact of change implementation on the operational environment
- measuring positive and negative impact
- analysis of positive and negative impact

- configuration of digital system impacted by the change:
  - current and proposed
- rollback planning - recovering to a previous stable configuration:
  - back-up methodology
  - local
  - cloud
  - disaster recovery planning
- reproducibility:
  - replicating change across other departments or businesses
  - test environment:
    - servers and software
- traceability:
  - responsibility
  - accountability
  - auditing
- document:
  - maintaining up-to-date information
  - recording of all decisions
  - retaining change documentation
  - user training manuals
  - version control

R1.7 Factors that drive change and a range of methods organisations can apply in response to change.

Internal factors:

- restructuring

What you need to teach

- expansion/growth
- downsizing
- new strategic objectives

External factors:

- political:
  - shift in governmental priorities (for example Brexit, international trade deals)
  - change in government
  - war
- economic:
  - meeting new funding/revenue streams
  - recession
  - inflation
  - consumer trends
- social:
  - change in human behaviour (for example birth rates)
  - market/social trends (for example rise in online shopping)
  - socioeconomic aspects
  - remote working
  - cultural expectations
- technological:
  - emerging technologies
  - innovation/efficiency
  - artificial intelligence
  - new payment methods
- legal/regulatory:
  - new legislation
  - changes/updates to legislation (for example national minimum wage, working hours, UK General Data Protection Regulation (UK GDPR)/Data Protection Act (DPA) 2018)
  - removal of European Union (EU) legislation
- environmental:

What you need to teach

- sustainability
- reduction in carbon footprint
- green energy
- digital/tech waste
- pandemic

- competitors:
  - new product/service
  - entering new markets

Methods to respond to change:

- new or amended:
  - policies (for example updated health and safety, due to changes in legislation)
  - business processes (for example implementation of new digital technologies)
  - products or services (for example innovation for new markets)
- new or improved digital systems for hardware and/or software (for example DVLA system, NHS referrals, online banking)
- training needs analysis
- restructuring of priorities and resources

R1.8 The steps organisations take to respond to change:

- planning for change:
  - setting budgets and timescales
  - communicating the change activity to all stakeholders
  - clarifying resources required (for example hardware, software, staffing)
- managing change implementation:
  - monitoring progress during implementation of change
  - maintaining quality of service during change
  - business acceptance and compliance with change
  - team upskilling and development to facilitate the change
  - communicating outcomes of change
  - post-project reviews
- reinforcing change:

What you need to teach

- reinforcement planning:
  - checking change is implemented
  - what steps to take if change isn't implemented quickly enough
- collating and analysing outcomes of change data
- monitoring change

R1.9 The measurable value of digital service to customers and end users.

Value to customers:

- efficient digital support for products and services
- timely response to customer queries or needs:
  - communicating expected response time
  - communicating any changes in response and reasons why
- financial savings (for example product/service price comparisons)
- access and engagement:
  - multi-platform multimodal format (for example social media, chat, email, phone)
  - time saving
- social integration for user and support community

Value to end users:

- efficient first line, second line and third line digital support to internal staff
- efficient resolution of end user needs
- effective hardware or software deployment

R1.10 The considerations and value of meeting customer and end user needs within a business context.

Considerations to meet customer and end user needs:

- customer or end user profile:
  - cultural awareness/diversity
  - inclusivity
  - accessibility
  - adhering to guidelines, policies and regulatory requirements
  - level of technical knowledge and skills (for example use of technical terminology)
- customer or end user issues:
  - problem type and pain points:

What you need to teach

- usability
- functionality
- training on new systems

- system or service response time
- system or service availability

Value of meeting customer and end user needs:

- increased financial benefit due to customer retention and satisfaction
- improved user experience
- reputational:
  - protection of brand reputation
  - brand awareness
  - positive media exposure
- quantitative and qualitative market research
- product development through product use analytics
- more sophisticated marketing allowing personalised and targeted advertisements for consumers
- positive third-party reviews (for example unboxings, meta critic, user reviews)

R1.11 Risks and implications within a business environment.

Risks:

- privacy:
  - potential loss of control over personal and business information
- security:
  - compromises to the confidentiality, integrity and availability of all business data
- non-compliance:
  - non-adherence to policies, procedures and legislation
- audience exclusion:
  - bias towards a particular demographic
- insufficient business resilience:
  - inability to adapt to disruptions
  - inability to adapt to change
- technical:

What you need to teach

- system not fit for business purpose
- doesn't meet user requirements

Potential impact of risks:

- lawsuits
- dismissal
- fines
- reputational/brand damage
- withdrawal of licence/rights to practise
- loss of job
- loss of business:
  - reduction in sales

R1.12 The purpose and applications of codes of conduct within a business.

Purpose and application:

- ensures that individuals and organisations operate within policies, procedures and legislation:
  - professional practice
  - industry standard
- describes accepted practice for individuals and organisations:
  - confidentiality
  - ethical principles
  - use of equipment and facilities
  - standard working practice
  - access permissions to data and systems
  - supports individual company values

Types of codes of conduct within a business:

- organisational codes of conduct (for example Google, Twitter, code of business conduct (COBC)
- professional codes of conduct (for example British computer society (BCS))
- governmental (for example Technology Code of Practice, Data Ethics Framework)

R1.13 Types of hacker and the implications of hacking and non-compliance with a code of conduct.

Types of hacker:

- white hat/ethical hacker:

What you need to teach

- working on behalf of businesses to test the security of systems or networks using ethical tools, techniques and methodologies
- has permission to engage in social engineering within agreed parameters
- feedback given to businesses on system or network vulnerabilities

- grey hat:
  - accesses systems or networks without malicious intent
  - discloses vulnerabilities to businesses or relevant authority
- black hat:
  - unauthorised access to systems or networks for malicious intent
  - compromises or shuts down security systems or networks
  - unauthorised access to passwords, financial information or other personal data
  - threat actors:
    - hacktivist – motivated by specific cause (for example animal rights)
    - organised crime syndicate – motivated by financial gain
    - nation state – motivated by political agenda

Implications of hacking and non-compliance:

- internal implications:
  - disciplinary action
  - loss of employment
  - restriction of potential employability
  - restricted privileges
- external implications:
  - loss of status with professional bodies
  - prosecution:
    - fines
    - imprisonment
  - reputational damage

Route core element 2: Culture

What you need to teach

The student must understand:

R2.1 How the increasing reliance on digital technology can cause ethical and moral impacts on business and society.

Impacts on business:

- impact on company culture:
  - changes in face-to-face communication (for example remote working, video conferencing)
  - increase in expected productivity and outputs
  - increase reach and scale
  - increase of staff monitoring
  - adaptive working practices
- autonomous operation:
  - dehumanisation of service:
    - loss of jobs
    - loss of human empathy in decision making
  - shift in skill requirements and skills redeployment

Impacts on society:

- loss of privacy:
  - digital footprint
  - surveillance
- changing behaviours:
  - social skills
  - scalable remote engagement, wider peer and professional networks
  - creation and curation of a digital identity
- communication access:
  - resistance to technological change
  - potential isolation:
    - transition to remote communication and services
    - due to lack of digital skills or technology
    - locations (for example limited mobile data coverage)

What you need to teach
○ improved access to information (for example educational, online employment searches, access to 24/7 advice - NHS) **R2.2 The impact of unsafe or inappropriate use of digital technology and mitigation techniques to reduce impact.** Impacts: • psychological: ○ cyberbullying ○ mental health ○ addiction (for example gambling, gaming, social media) ○ stress • physical: ○ posture ○ eye strain ○ repetitive strain injury (RSI) ○ reduction of physical activity ○ disturbed sleep patterns Mitigation techniques: • regulate use of digital technology (for example effects on sleep patterns, effects on mental health, screen breaks) • report misuse to relevant authority (for example platform owners, police) • display screen equipment (DSE) and workstation assessment: ○ equipment (for example footrest, back support, screen filters) • self-exclusion (for example gambling website/app)

Route core element 3: Data

What you need to teach
The student must understand: **R3.1 The fundamental characteristics of data.** Data types:

What you need to teach

- numeric
- text
- media
- geospatial
- temporal
- logical

Sources of data for organisations:

- internal:
  - sales data
  - marketing data:
    - engagement data
  - financial data
  - employee data
  - customer data
  - usage data:
    - traffic data
- external:
  - public (for example open data, repositories)
  - government (for example data.gov.uk)
  - suppliers
  - competitors
  - sector/industry
  - market research
  - repositories

Storing data:

- on-premises:
  - internal databases
  - file structures and formats
  - hard drives:
    - solid state drive (SSD)

What you need to teach

        - hard disk drive (HDD)
      - portable storage devices
      - file servers
      - network-attached storage (NAS) devices
      - storage area network (SAN)
  - cloud storage:
      - file storage
      - object storage
      - block storage
      - elastic cloud/scalable storage
      - cloud-based database services

R3.2 The fundamental functions of information systems and the application of data:

- input - data inputted in preparation for processing
- storage - recording and retention of data on an appropriate format:
    - create/store - retain data records for future use or compliance
    - organise - restructure and rank data in a specific order
- processing - transforming data into meaningful output:
    - analyse - business/digital insight through search queries/criteria
    - update - ensuring data records are up to date
    - remove - removal of data entries where appropriate
    - integrate - integrate different sets of information together
- output - data generated by the information system:
    - read/search - identify and find specific information
    - insight - gain from processing to support decisions
- feedback loop - a system structure that allows output to influence future input

R3.3 The concepts and tools of data modelling.

Concepts:

- hierarchical database model - data organised and accessed in hierarchy structure
- network model - data organised and accessed through nodes and links
- entity relationship model - data organised and accessed through use of relationships

What you need to teach

Tools and their application:

- entity relationship diagram (ERD):
  - used to design relational databases
- data flow diagram (DFD):
  - level zero and level one
  - visual representation of information flow within a system

R3.4 The concepts involved in data entry and maintenance.

Data entry:

- assign common data types to screen input boxes:
  - numeric:
    - integer
    - float
    - double
  - text:
    - strings
    - char
  - Boolean
    - true/false
- reducing risk of data entry errors:
  - validation - check that user-entered data is sensible and in correct format
  - verification - check that user-entered data is accurate
- privacy:
  - compliance with standards and legislation for usage and storage

Data maintenance:

- user:
  - editable data screens for permitted data changes
- system administrator:
  - privileges to allow direct changes to data:
    - user level
    - user group level

What you need to teach

- file level

Business resource considerations for data entry and maintenance:

- operational:
  - time
  - staffing
- financial:
  - budget
  - estimating and forecasting
- technological:
  - hardware
  - software
  - storage

R3.5 Characteristics of data formats and importance for analysis.

Data formats:

- file-based structure:
  - data held within one file
  - consistent set of attributes, data types and validation
  - context is held within the file
  - data is referenced within the file
  - data stored in flat file format
- directory-based structure:
  - data held across multiple files
  - contains multiple attributes, data types and validation
  - context held within the file and the structure
  - relational data is referenced across multiple files
  - datasets are extracted from system and filtered
  - data can be structured in a hierarchy system
  - allows multiple data owners and sources
- relational database systems:
  - data organised using normalisation to reduce redundancy

What you need to teach

- data connect by relationships
- structured query language (SQL)/data processing language
- server-client implementation

Importance for analysis:

- easier to query
- easier to keep up to date
- supports with drawing conclusions
- allows sharing of data

R3.6 Methods of presenting and visualising data and their suitability for application.

Presenting data:

- reports
- digital slides
- webinars
- extended reality (XR):
  - virtual reality (VR)
  - augmented reality (AR)
- video
- sound
- animation

Visualising data:

- graphs (for example bar, line)
- charts (for example pie, funnel, area)
- data tables
- dashboards
- infographics
- maps
- heat maps

Suitability for application:

- formal or informal
- meeting requirements:

What you need to teach

- brief
- audience
- level of technical knowledge and skills (for example use of technical terminology)

R3.7 Applications of data within an organisation:

- analysis:
  - identifying trends and patterns
  - monitoring performance:
    - staff
    - product/service usage
  - forecasting (for example predictive analytics)
  - informing decision making
- marketing:
  - customer profiles
  - targeting customers
  - direct promotion
- operational management:
  - monitoring and control of operations
  - setting and monitoring of KPIs
  - service improvement

R3.8 Types of data access management across platforms within in a digital environment.

Types of data access management:

- user access controls:
  - physical access
  - remote access
  - permissions
  - authentication
- application programming interface (API):
  - set of rules or specifications
  - allows interface between software

R3.9 Types and application of access control methods:

What you need to teach
• role-based access control (RBAC) - restricts or allows access to resources based on the role of a user • attribute-based access control (ABAC) - restricts or allows access based on attributes or characteristics • mandatory access control (MAC) - restricts or allows access based on a hierarchy of security levels • discretionary access control (DAC) - restricts or allows access based on resource owner preference

Route core element 4: Digital analysis

What you need to teach
The student must understand: **R4.1 The characteristics and applications of algorithms in digital analysis:** • algorithms - a process or set of clearly defined rules followed to support calculations or problem solving. Characteristics of algorithms: • finiteness - finite number of steps • unambiguous - steps must be clear and lead to one meaning • clearly defined inputs and outputs • logical sequencing of steps • iteration - repetition of steps until results achieved • selection - input leading to choice of step • structured English Applications of algorithms for digital analysis: • automate calculations to improve efficiency of a process • design a step by step solution to solve a problem • supports machine learning for data analysis **R4.2 The process of computational thinking and tools applied in problem solving and algorithm design.** Process of computational thinking: • decomposition - breaking down a complex problem or system into manageable components • pattern recognition - identification of patterns within problems

What you need to teach

• abstraction - analyse information, filter and remove unnecessary detail
• action:
  ○ sequence - order of processes
  ○ selection - execution only when conditions met
  ○ iteration - repetition until conditions met
Tools for problem solving and algorithm design:
• decomposition diagram
• flowchart
• pseudo code

Route core element 5: Digital environments

What you need to teach

The student must understand:
R5.1 Components of physical computing systems and their applications:
• chassis – to house the components of a system
• optical drive – CD/DVD reader and writer
• mainboard/motherboard – allows internal devices to communicate
• central processing unit (CPU) – main computing part of unit
• random access memory (RAM) – volatile temporary storage
• graphics processing unit (GPU) – enables the ability for output to display unit
• storage (for example SSD/HDD) – used to store data
• fans – used to maintain the temperate of computing system
• peripherals:
  ○ screen
  ○ keyboard
  ○ mouse
R5.2 Types and applications of networks, hardware and software, and the functions of internet of things (IoT).
Networks:

What you need to teach

- personal area network (PAN) – single peer-to-peer connectivity (for example wireless headset to a computer)
- local area network (LAN) – interconnected devices belonging to the same organisation within one area (for example within an office building)
- metropolitan area network (MAN) – 2 or more interconnected LANs within a small geographical area (for example buildings at opposite ends of town)
- wide area network (WAN) – many interconnected LANs over a large geographical area (for example the internet)
- virtual private network (VPN) – used to create a secure connection between a device and a network or between different networks (for example working from home device connecting to corporate network using provided VPN)

Hardware:

- switch – provides connectivity to multiple network devices
- router – used to route traffic between networks
- network interface devices:
  - peripheral component interconnect (PCI) network cards
  - universal serial bus (USB) network cards
- cabling:
  - copper
  - fibre optic
- wireless access point – used to deliver wireless networking to capable devices:
  - servers

Software:

- system software:
  - operating systems (OS):
    - proprietary (for example Microsoft Windows, Apple MacOS)
    - open source (for example Linux, Unix)
    - network operating system (NOS)
  - file management utilities
- application software:
  - productivity suites (for example Video editing)
  - protection software (for example firewall, anti-virus)

What you need to teach

- web browsers (for example Chrome, Firefox, Edge)

Function of IoT:

- devices dedicated to basic services, data collection, manipulation or analysis, requiring servers to process the task and information:
  - data collection, analysis and manipulation:
    - edge computing
    - sensors (for example temperature sensors, vibration sensors)
  - network utilisation
  - use within an industrial context
  - use within a smart city context
  - use within a domestic context (for example, home-based)

R5.3 The types and applications of protocols used to create networks and network referencing models.

Protocols:

- web protocols – applied to web communication (for example retrieving websites):
  - hypertext transfer protocol (HTTP)
  - hypertext transfer protocol secure (HTTPS)
- mail protocols – the ability to send and receive emails:
  - simple mail transfer protocol (SMTP)
  - post office protocol (POP)
  - internet message access protocol (IMAP)
- routing protocols – used to route data between networks:
  - routing information protocol (RIP)
  - open shortest path first (OSPF)

Network referencing models:

- open systems interconnection (OSI):
  - used in troubleshooting - standardised approach to computing system with an underlying structure characterised by 7 layers:
    - physical
    - data

What you need to teach

- network
- transport
- session
- presentation
- application

- transmission control protocol, internet protocol and user datagram protocol (TCP/IP/UDP):
  - set of communication protocols used by the internet and computer systems characterised by 5 layers:
    - physical
    - data
    - network
    - transport
    - application
      - file transfer protocol (FTP)
      - secure file transfer protocol (SFTP)
      - dynamic host configuration protocol (DHCP)
      - domain name system (DNS)

R5.4 The components and benefits of virtual computing systems.

Components:

- virtual machines (VMs):
  - clients (for example virtual PC, virtual switch, virtual router)
  - servers
- hypervisor:
  - type 1 (for example Microsoft Hyper-V, VMware ESXI)
  - type 2 (for example virtual PC, virtual server, VMware Workstation)

Benefits:

- more cost effective in larger digital environments
- easier to manage and maintain larger environments
- resilient (for example clustering)
- environmental (for example lower carbon footprint)

What you need to teach

- disaster recovery options
- efficient testing environments
- education and training platform

R5.5 The types, services and benefits of cloud computing.

Types of cloud:

- private
- public
- community
- hybrid

Cloud services:

- (infrastructure as a service (IaaS):
  - applications, OS and data are client managed
  - servers, network infrastructure and storage are vendor managed
- platform as a service (PaaS):
  - applications and data are client managed
  - servers, network infrastructure, storage and OS are vendor managed
- function as a service (FaaS):
  - functions are client managed
  - network infrastructure vendor managed
- software as a service (SaaS):
  - access to application software
  - no installation or maintenance
  - client only managed user
  - rest is managed by the vendor
- everything as a service (XaaS):
  - outsourcing all organisational digital requirements

Benefits of cloud computing:

- cloud portability - ability to quickly and easily move services
- cloud sourcing - purchasing services from a third party using the cloud
- elastic cloud - on-demand services which can be scaled to meet needs

What you need to teach

- storage - no physical limitations on storage capacity
- cost effective - efficiencies of scale

R5.6 The methods and benefits of creating a resilient digital environment.

Methods of creating a resilient digital environment:

- installation of software updates/upgrades
- replacement and removal of hardware
- adding redundancy into systems
- decommission and remove legacy hardware and software
- device hardening:
  - removing unneeded applications, ports, permissions and access
  - limiting user account functions
- maintaining effective back-up systems:
  - on-premises
  - off-site/remote
  - cloud
- appropriate and reviewed standard operating procedures (SOPs)
- structured staff training for:
  - new hardware/software
  - staff inductions
  - new and updated policies and procedures

Benefits of a resilient digital environment to the organisation:

- increased security:
  - secure transfer of data
  - secure storage of data
  - reduced system vulnerabilities
  - reduced probability of targeted cyber attacks
- increased reputation and profile:
  - customer confidence
  - protects brand image
- lower downtime of services

Route core element 6: Diversity and inclusion

What you need to teach

The student must understand:

R6.1 The principles of digital inclusion, and legislation relating to equality and diversity.

Digital inclusion principles:

- ensuring no one is disadvantaged by a digital system
- checking for bias within datasets before use
- access:
  - technology
  - connectivity
  - conforming to codes of best practice (for example Web Content Accessibility Guidelines (WCAG))
- technical knowledge and skills

Legislation:

- the Equality Act 2010:
  - direct discrimination
  - indirect discrimination
  - 9 protected characteristics:
    - age
    - disability
    - gender reassignment
    - marriage and civil partnership
    - pregnancy and maternity
    - race
    - religion or belief
    - sex
    - sexual orientation
- the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- the Equality and Human Rights Commission (EHRC) Statutory Code of Practice for 'Services, Public Functions and Associations' under the Equality Act

R6.2 The business benefits of diversity and inclusion:

What you need to teach

- more innovative products
- greater appeal to potential employees
- inclusive products
- ability to connect authentically to black, Asian and minority ethnic (BAME) groups
- reduce risk of reputational damage from non-inclusive products

R6.3 Approaches to addressing demographic imbalance in the digital sector:

- increasing cultural awareness of different types of bias
- application of digital inclusion principles
- inclusion by design of digital technologies and systems
- government initiatives
- inclusive recruitment

R6.4 How digital inclusion affects individuals and organisations in the digital sector.

Effects of digital inclusion:

- individuals:
  - inclusive services
  - increased career opportunities
  - enhanced access and connectivity to digital technology
  - greater social mobility
  - greater scope of communication and collaboration
- organisations:
  - greater variation in employment demographics
  - enhanced connectivity in more remote communities
  - creating and expanding commercial markets
  - greater profitability
  - more innovation
  - more skilled workforce
  - more inclusion resulting in greater employee retention

Adverse effects when principles of digital inclusion are not applied:

- individuals:
  - reduced quality of life

What you need to teach
○ social isolation ○ restriction in services ○ financial loss • organisations: ○ lack of skilled people for required roles ○ lack of innovation ○ breach of legalisation and regulations ○ restriction in services ○ financial loss ○ reputational damage ○ breach of regulations

Route core element 7: Learning

What you need to teach
The student must understand: **R7.1 The advantages of personal and professional development in the digital sector:** • increased industry and sector competence and knowledge • increased employability potential and employment security • achieving accreditation to specific professional disciplines • maintaining currency and relevance to industry • achieving access to specific professional bodies • knowledge of and adherence to industry standards **R7.2 Areas of emerging technology and innovative applications within a commercial and domestic context:** • new mediums for storing information (for example DNA data storage) • quantum computing/internet and quantum cryptography • IoT • artificial intelligence

What you need to teach

- XR:
  - AR
  - VR
  - mixed reality (MR)
- blockchain
- application of 3D printing
- 5G
- drones
- green computing

R7.3 Types of reflection and creativity techniques and how they influence practice within the digital sector.

Reflection techniques:

- Kolb's Experiential Learning Cycle - 4 stages of reflecting on experience:
  - concrete – learning from feelings or experiences
  - reflective – learning from watching
  - abstract – learning from reflections and thinking
  - active – learning from practical application of ideas
- Gibbs' Reflective Cycle - 6 stages of reflecting on experience:
  - description – recording key components of the task or project (for example expected outcome, actions taken, data of occurrence)
  - feelings – recording reactions and feelings
  - evaluation – reviewing positive and negative actions and outcomes
  - analysis – reflecting on process and outcomes of task or project
  - conclusion – summarising actions and outcomes from task or project
  - action plan – recording future plans and areas for improvement
- Boud, Keogh and Walker's model - 3 stages of reflecting on practice:
  - experience – considering behaviour, ideas and feelings
  - reflective – returning to and re-evaluating experiences
  - outcomes – gaining new perspectives or changes in behaviour creativity technique

Creativity technique:

What you need to teach

- design thinking:
  - identify users' needs
  - empathise with users' needs
  - define the problem
  - hypothesise
  - map/challenge assumptions
  - ideate - create ideas that might solve the problem
  - prototype feedback loop
  - conduct qualitative research with users
  - validate/disprove assumptions
  - iterate prototype based on research

R7.4 Sources of knowledge within the digital sector and the factors that need to be considered when assessing the reliability and validity of a source.

Sources of knowledge:

- forums
- textbooks
- academic papers
- white papers
- supplier literature
- search engines
- websites
- blogs
- wikis
- social media
- conferences
- developer kits
- e-learning
- subject matter expert

Reliability and validity factors:

- author expertise

What you need to teach
• bias • evidence • subjectivity • context • intended audience • date of publication • corroboration of sources • citations

Route core element 8: Legislation

What you need to teach
The student must understand: **R8.1 Legislation and regulation requirements applied across sectors in a digital context.** UK requirements: • Health and Safety at Work etc Act 1974 (including Work at Height Regulations 2005, Manual Handling Operations Regulations 1992, Management of Health and Safety at Work Regulations 1999, Health and Safety (Display Screen Equipment) Regulations 1992): o key features: ▪ adequate training of staff ▪ adequate welfare provision for staff at work ▪ a safe working environment that is properly maintained ▪ suitable provision of relevant information, instruction and supervision • Investigatory Powers Act 2016: o key features: ▪ enhances powers for law enforcement and security agencies to obtain and intercept communications and data ▪ highlights the way in which new powers are authorised and overseen ▪ ensures powers are fit for the digital age • Freedom of Information Act 2000:

What you need to teach

- key features:
  - public sector are required to publish information
  - members of the public are entitled to request information from public authorities

- Computer Misuse Act 1990
  - key features:
    - governs unauthorised access to computer programmes or data
    - governs unauthorised access with further criminal intent
    - governs unauthorised modification of computer material
- Digital Economy Act 2017:
  - key features:
    - regulation of communication infrastructure and services
- Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations 2018:
  - key features:
    - to make clear the level of accessibility required across websites or applications
- Copyright, Designs and Patents Act 1988:
  - key features:
    - protects intellectual property rights
    - enables control over the ways in which material can be used
- The Waste Electrical and Electronic Equipment Regulations 2013:
  - key features:
    - governs the safe and environmentally responsible disposal of electrical equipment
- Human Rights Act 1998:
  - key features:
    - governs an individual's right to privacy
    - governs surveillance
- Data Protection Act 2018:
  - key features:
    - implementation of UK General Data Protection Regulation (UK GDPR)

International requirements:

- European Convention on Human Rights (ECHR) - Article 8:

What you need to teach

- key features:
  - the right to respect for family and private life
- UK General Data Protection Regulation (UK GDPR):
  - key features:
    - lawfulness, fairness and transparency
    - purpose limitation
    - data minimisation
    - accuracy
    - storage limitation
    - integrity and confidentiality (security)
    - accountability
    - data security
- Electronic Communications Privacy Act (ECPA) 1986 - USA:
  - key features:
    - protect wire, oral and electronic communications while in transit
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act 2003 - USA:
  - key features:
    - sets rules for commercial emails and gives rights to recipients (for example to unsubscribe)

R8.2 The role of criminal law, industry standards and professional codes of conduct in a digital context.

Criminal law:

- national:
  - maintains order
  - resolves disputes
  - protects individuals and property
  - safeguards civil liberty
- international:
  - governs offences committed outside of the UK

Industry standards and professional codes of conduct:

- compliance

What you need to teach

- facilitating competition within industry
- promoting innovation
- providing interoperability between new and existing systems
- ensuring security
- ensuring transparency of sectors

R8.3 Where to access industry standards and professional codes of conduct in a digital context.

Industry standards:

- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF):
  - Request for Comments (RFC)
- Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA)
- British Standard (BS)
- Institute of Electrical and Electronics Engineers (IEEE)
- Payment Card Industry Security Standards Council (PCISSC)

Professional codes of conduct:

- British Computer Society (BCS)
- Institution of Analysts and Programmers (IAP)
- Chartered Institute of Information Security (CIISec)

R8.4 The importance of keeping up to date with UK and international legislation and regulations and potential consequences to businesses across sectors of being non-compliant.

Importance:

- protection for business
- protection for customer
- avoiding consequences of non-compliance

Potential consequences of non-compliance:

- financial:
  - fines
  - loss of business/income
- legal:
  - prosecution

What you need to teach

• professional:
  ○ termination of employment
  ○ revoked responsibilities
• reputational:
  ○ brand damage
  ○ customer perception
• sector specific consequences (for example health, education, retail, hospitality)

Route core element 9: Planning

What you need to teach

The student must understand:
R9.1 The principles of project planning.
Identification of project aims and objectives:
• project scope:
  ○ user/client requirements
  ○ business case
• expected outcomes
• stakeholder map
• timeline and deadlines
• linked to organisational strategic objectives
Resource requirements:
• people and skills
• estimates and costings
• venues/premises
• facilities
• equipment
• hardware and software
• stakeholder engagement

What you need to teach
Budgeting: • accurate estimating and forecasting • financial contingency planning • reasonable and documented assumptions Cost-benefit analysis: • viability of project • quantifying the intended deliverables Project lifecycle: • timing and scheduling (for example communication plan, reporting schedules) • work packages to break down deliverables • milestones • prioritisation identification • dependencies identification Risk and issues management: • identification • probability • impact • prioritisation • analysis • mitigation controls • contingency planning Quality management: • monitoring of project deliverables • quality assurance • quality control • review and audit
R9.2 The consequences of ineffective project planning: • under-resourced • escalating costs • exceeding timeframes

What you need to teach
• unable to deliver outcomes • negative environmental impact • health and safety risks • scope creep **R9.3 The application of project planning techniques in a business context.** Techniques: • programme evaluation review technique (PERT) – used to identify and estimate timescales of project activities • critical path analysis (CPA) – used to identify key tasks within a project • work breakdown structure (WBS) – used to break down the scope of a project into manageable work packages • responsible, accountable, consulted or informed (RACI) matrix - used to manage and categorise stakeholders • must have, should have, could have, won't have (MoSCoW) – used to prioritise the requirements of a project

Route core element 10: Security

What you need to teach

The student must understand:
R10.1 Types of confidential company, customer and colleague information:
• human resources:
  ○ salaries
  ○ benefits/perks
  ○ employment data:
  ▪ recruitment
  ▪ termination
  ▪ appraisals/disciplinary
  ○ medical information
• commercially sensitive information:

What you need to teach
○ sales revenue ○ trade secrets ○ profit margins ○ client/customer details ○ stakeholder details ○ contracts ○ intellectual property (IP) • access information: ○ passwords ○ multi-factor authentication ○ email accounts ○ phone numbers ○ access codes **R10.2 The importance of maintaining and the consequences of not maintaining confidentiality, integrity and availability (CIA).** The importance of maintaining CIA: • maintains compliance • maintains trust with internal and external stakeholders • promotes positive brand image • avoids security risks and unauthorised access The consequences of not maintaining CIA: • financial: ○ regulatory fines ○ refunds/compensation to customers ○ loss of earnings • legal: ○ lawsuits ○ termination of contract • reputational: ○ loss of clients

What you need to teach

- damage to brand

R10.3 The technical and non-technical threats that may cause damage to an organisation:

- technical:
  - botnets
  - denial-of-service (DoS)
  - distributed denial-of-service (DDoS)
  - hacking:
    - cross-site scripting (XSS)
    - password-cracking software
    - SQL injection
  - malware:
    - viruses
    - trojans
    - worms
    - remote access Trojans (RATs)
    - key loggers
    - ransomware
    - spyware
    - adware
  - malicious spam:
    - phishing
    - spear phishing
    - smishing
    - vishing
    - pharming
  - buffer overflow
- non-technical:
  - human error
  - malicious employees
  - disguised criminals

What you need to teach

- natural disaster (for example flooding)
- social engineering

R10.4 The technical and non-technical vulnerabilities that exist within an organisation:

- technical:
  - inadequate encryption (for example weak or outdated)
  - out of date:
    - software
    - hardware
    - firmware
- software no longer supported by supplier:
  - compatibility of legacy systems
  - fail-open electronic locks
  - weak passwords (for example default passwords)
  - missing authentication and authorisation
  - exploitable bugs/zero-day bugs
- non-technical:
  - employees:
    - not following policies and procedures
    - competency levels of staff
    - lack of recruitment screening
    - poor data/cyber hygiene (for example not archiving dormant staff accounts and access)
  - physical access controls:
    - inadequate security procedures:
      - door access codes not changed regularly
      - using simple access codes and reusing access codes (for example 1234)
      - no monitoring of access to secure areas
    - unnecessary staff access to secure areas

R10.5 The potential impacts of threats and vulnerabilities on an organisation:

- loss of sensitive information
- unauthorised access to the system or service

What you need to teach

- overload of the system to affect a service
- corruption of a system or data
- damage to system operations
- disclosure of private information and credentials
- unauthorised access to restricted physical environment
- essential security updates not installed

R10.6 Risk mitigation controls to prevent threats to digital systems:

- National Cyber Security Centre (NCSC) Cyber Essentials:
  - firewall to secure internet connections
  - choose most secure settings for devices and software
  - control access to data and services
  - protection from viruses and malware
  - up-to-date software and devices
- anti-virus and anti-malware software
- firewalls:
  - software
  - hardware
- intrusion detection and prevention systems
- encryption:
  - purpose
  - process
  - protocols
- user access, policies and procedures:
  - permissions
  - IT user policies
- staff training and CPD (continuous professional development):
  - human firewall
- back-ups:
  - full
  - incremental

What you need to teach
- differential   - software and system maintenance: - importance of latest software updates   - scheduled maintenance   - interruption to service   - air gaps   - honeypot   - virtual private networks (VPNs)   **R10.7 The process and protocols of internet security assurance.** Processes: - installation and configuration of firewalls: - inbound and outbound rules: - traffic type rules   - application rules   - destination and source rules   - network segregation: - VLANs   - physical network separation   - offline networks   - network monitoring   - removable media controls   - anti-virus   - managing user privileges   - penetration/vulnerability testing: - port scanning   - SQL injecting testing   - Secure Sockets Layer (SSL)/Transport Layer Security (TLS) scanning   Protocols: - VPN   - IPSec VPN

What you need to teach
○ SSL VPN • SSL/TLS • SFTP - secure file transfers • secure shell (SSH) - secure connection to devices • HTTPS **R10.8 The interrelationship of components required for an effective computer security system.** Components: • confidentiality, integrity and availability (CIA) • identification, authentication, authorisation and accountability (IAAA) • risk management: ○ threats ○ vulnerabilities ○ impact ○ probability ○ mitigation

Route core element 11: Testing

What you need to teach
The student must understand: **R11.1 The purpose of testing digital components.** Purposes of testing: • functionality • usability • compatibility • accessibility • customer/client/end user satisfaction • fault-finding and de-bugging • impact assessment

What you need to teach
• efficiency of individual components • review accuracy of data • ensuring desired outcome (for example service or product) • performance monitoring Digital components: • software • hardware • data • interfaces • test scripts **R11.2 The process of applying root cause analysis to problems.** • define the problem • collect data relating to the problem • identify what caused the problem • prioritise the causes • identify solutions to the underlying problem • implement the change • monitor and sustain **R11.3 Testing methods and their application in the digital sector:** • concept testing: o scoping and validating requirements o informing decisions before committing time and resources to a project • usability/audience testing: o testing whether the functionality fulfils the desired outcome o identifying usability problems o determining user satisfaction with product • stress testing: o testing whether a system can function with expected demand by replicating real world load • penetration testing: o determining vulnerabilities in a controlled environment

What you need to teach
○ authorised attack on systems • black box testing: ○ testing inputs and outputs against expected results ○ measuring the functional requirements of a system • white box testing: ○ testing internal structure of process flows

Route core element 12: Tools

What you need to teach
The student must understand: **R12.1 The application of digital tools and methods in a business context.** Presentation tools: • slide/page presentation software: ○ product demo ○ sales meetings ○ training ○ promotion and marketing (for example expos, speaking at events) • digital infographics: ○ posters ○ leaflets • graphs: ○ sales trends ○ market comparisons • dashboards: ○ display/monitor KPIs ○ management information ○ business intelligence Project management methodologies:

What you need to teach

- agile - promotes adaptability through different iterations:
  - frameworks:
    - Scrum
    - Kanban
    - lean
- waterfall - definitive stages that follow on from each other
- spiral
- rapid application development (RAD)

Project management tools and their application:

- Gantt charts - used to measure time scales and milestones of a project
- flowcharts - outlines the logical process for workflow
- stakeholder power interest matrix - visual representation to assess stakeholder priority
- budget sheets - organise and document finances over project lifespan (for example forecasting, expense tracking)

Evaluation tools:

- marketing analytics tools:
  - search analytics
  - social media analytics
- financial analytics tools
- reporting tools
- data mining

R12.2 The application of collaborative communication tools and technologies in business.

Communication tools and technologies:

- intranet
- shared workspaces:
  - online
  - on-premises
- shared documents
- discussion threads
- online shared storage

What you need to teach

• mark-up:
  ○ track changes
  ○ comments
• video conferencing

The pathway core: Core knowledge and understanding across digital support services

Pathway core element 1: Careers within the digital support services sector

What you need to teach

The student must understand:

P1.1 The range of responsibilities, job roles and skills required of professionals in digital infrastructure:

- responsibilities:
  - installing, testing and maintaining infrastructure components and systems
  - maintaining the efficiency and effectiveness of an organisation's infrastructure
  - communicating digital infrastructure updates and scheduled system changes to end users
  - proactive management of digital services using structured techniques and digital tools to ensure optimum availability
  - recovery and restoration of digital services
  - performance optimisation of hardware, software and network system
  - applying security measures to digital devices and networks
  - incident/problem detection, support and escalation (for example escalation to 3rd line technical support)
  - working to relevant legislation, standards and industry best practice
  - system design and documentation to organisational standards
- job roles:
  - service desk roles (for example technician/operative)
  - 1st line to 4th line (for example analyst/engineer)
  - network engineer
  - server engineer
  - infrastructure technician
- skills:
  - analytical thinking and problem solving
  - using digital monitoring and diagnostic tools:
    - logging and service management systems
    - manage social media (for example wikis, messages)

What you need to teach

- communicating effectively with technical and non-technical staff
- project management and planning:
  - prioritisation of tasks and workload
- collaboration and working as part of a team
- continuous learning, improving and upskilling

P1.2 The range of responsibilities, job roles and skills required of professionals in network cabling:

- responsibilities:
  - installing, termination, testing and certification of copper and fibre network cable infrastructure
  - maintenance of copper and fibre optic cabling
  - identify, locate and repair faults in copper and fibre optic network cabling
  - installation of equipment cabinets, fixtures/fittings and rack-mounting equipment
  - applying physical security measures to network cabling and infrastructure
  - carry out a risk assessment (for example health and safety risk assessment)
  - working to relevant legislation, standards and industry best practice
  - production of clear documentation showing cable route maps, testing and acceptance
  - updating asset registers when physical equipment is deployed
  - updating maintenance logs when equipment is repaired or updated
  - use of service management tools and systems to maintain efficiency and effectiveness through good practice, processes and procedures
- job roles:
  - structured cabling installer/engineer (for example telephony, fibre, data)
  - network surveyor
  - network analyst
  - network installation engineer
- skills:
  - manual handling
  - working at height
  - ability to interpret and follow instructions and plans
  - adaptable approach to work
  - project management and planning

What you need to teach

- prioritisation of tasks and workload
- ability to work alone or as part of a team
- customer service skills
- continuous learning, improving and upskilling

P1.3 The range of responsibilities, job roles and skills required of professionals in digital support:

- responsibilities:
  - providing digital support required by businesses of all sizes and in all sectors
  - identifying the difference between digital application requirements and digital service requirements of users:
    - digital application requirements:
      - supply of software
      - troubleshooting application issues
      - storage quota
    - digital service requirements:
      - information and data access
      - loaning of equipment
      - helpdesk support
      - multi-platform support
  - supporting business needs with appropriate digital services (for example hardware and software)
  - providing digital service by supporting end users to access and operate systems
  - providing 1st line desk side and remote technical support for computer hardware or software for internal and external customers
  - communicating digital support updates and scheduled system changes to end users
  - training end users on new digital applications and systems
  - maintaining an up-to-date asset register and configuration management database
  - incident response, resolution and problem management
  - escalation of issues to technical and external support
  - working to relevant legislation, standards and industry best practice
  - updating and maintaining a knowledge base with known fixes and procedure documentation
  - use of service management tools and systems to maintain efficiency and effectiveness through good practice processes and procedures

What you need to teach

- job roles:
  - 1st line support analyst
  - helpdesk analyst
  - service desk analyst
  - support desk analyst
  - IT support technician
  - desktop support technician
  - digital applications support specialist
- skills:
  - analytical thinking and problem solving
  - using logging systems, digital monitoring and diagnostic tools
  - prioritisation of tasks and workload
  - communicating effectively with technical and non-technical users
  - active listening
  - collaboration and working as part of a team
  - customer service skills
  - continuous learning, improving and upskilling

P1.4 Integrated digital communications responsibilities required in digital support services:

- installing, testing and maintaining integrated digital communications systems and networks (for example telephony, video, instant messaging, email)
- managing availability of integrated digital communications systems
- network configuration, monitoring and optimisation of network performance for communications systems
- applying security measures to integrated digital communications systems and networks
- system design and documentation of organisational standards

P1.5 The types of organisations where digital support services roles exist:

- public:
  - education (for example schools, colleges)
  - government (for example local authority, embassies)
  - healthcare (for example NHS hospitals, surgeries)

What you need to teach
○ emergency services • private: ○ telecommunications (for example BT Openreach, Sky, Virgin Media) ○ IT network installers (for example BT Openreach) ○ IT technical specific (for example Microsoft, IBM) • voluntary: ○ charities (for example British Heart Foundation, Cancer Research, RSPCA) ○ trusts (for example National Trust, Woodland Trust) ○ foundations (for example BBC, Children in Need) **P1.6 The routes into digital support services:** • further education (for example vocational specific) • apprenticeships/work-based learning • higher education (for example degree) • professional/vendor qualifications and employer/industry recognised courses (for example CompTIA, Cisco, BCS) • professional recognition (for example progressing within an organisation)

Pathway core element 2: Communication in digital support services

What you need to teach

The student must understand:

P2.1 Types of communication methods applied to digital support services:

- written – formal and informal
- verbal – formal and informal
- non-verbal (for example body language)

P2.2 Types of communication formats and techniques applied to digital support services:

- formats:
  - telecommunication
  - email
  - incident tickets
  - notifications (for example system updates)
  - instant messenger
  - forum
  - face-to-face conversation
  - digital conferencing
  - presentation
- techniques:
  - troubleshooting
  - active listening
  - reading of body language and facial expressions
  - use of open questioning
  - negotiation
  - conflict handling/de-escalation
  - use of clear and concise language (for example terminology based on audience)

P2.3 Factors to consider when communicating to an audience in a digital support services context:

- target audience
- size of audience
- level of digital knowledge, literacy and experience of the audience

What you need to teach

• requirements of audience:
  ○ communication format
  ○ level of detail
P2.4 The relation and interaction between digital support services and technical and non-technical customers/clients/end users:
• verbal support in person or over the phone
• written updates by email or added to a support ticket or system which the user can view
• classroom or individual training and support
• remote support
• screen sharing
• messaging technology
• pre-recorded topic-based e-learning
P2.5 The relation and interaction between digital support services and technical and non-technical managers:
• providing direction, support and route for escalation
• written progress reports
• escalation of issues through a support ticketing system or via email
• verbal updates on progress
• presentation given for a project proposal
P2.6 The relation and interaction between digital support services and technical and non-technical peers/colleagues:
• support and knowledge sharing (for example best practice)
• information, advice and guidance:
  ○ technical training and resources (for example user guides)
• digital conferencing for collaborative working

Pathway core element 3: Fault analysis and problem resolution

What you need to teach

The student must understand:

P3.1 Fault analysis tools and their applications to identify problems:

- system alerts – to flag when a system condition is outside predetermined parameters
- activity/error logs – record of all interactions and events within network systems
- live traces – to identify any network traffic or activity in real-time
- dashboards – a consolidated visual representation of system condition and performance

P3.2 The purpose and application of organisational frameworks for troubleshooting and problem management:

- problem identification – identify and isolate faults using diagnostic and analytical tools to establish the probable cause
- logging – review fault history, identifying potential trends and issues
- action plan – plan or strategy for repair, restoration and prevention of further issues
- escalation – to an appropriate manager, specialist or external third party
- solution implementation – implement required changes to fix and restore services
- problem closure and review – notify user and document any configuration changes

P3.3 Root cause analysis approaches and their applications within problem management:

- the 5 ‘whys’ – an iterative questioning technique to identify underlying issues and causes
- fishbone diagram – to establish cause and effect by grouping possible causes into various categories
- failure mode and effects analysis (FMEA) – identifies which parts of the process or system are faulty
- event tree analysis (ETA) – to identify consequences of a single failure for the overall system reliability
- Pareto chart – to identify the significance of a number of factors on a particular fault or problem
- scatter diagram – to identify a relationship between 2 factors or variables

P3.4 The principles of incident management (for example Information Technology Infrastructure Library (ITIL®)) models in the context of digital support services:

- detection:
  - report and record the incident
  - investigate and perform analysis to determine the extent and cause of the incident
  - prioritise and categorise the incident
- response:

What you need to teach
○ identify an owner who will have responsibility for the incident ○ resolve the issue and restore service ○ record incident resolution and applied changes • intelligence: ○ record lessons learned, fixes and procedure updates ○ perform in-depth investigation and analysis to identify the root cause of the incident (for example forensic analysis) ○ share lessons learned as input to continual improvement and to reduce risk of incident repetition **P3.5 The requirements for external reporting of faults and problem resolution:** • to comply with relevant legislation, regulations and external standards (for example report to the Information Commissioner's Office (ICO)) • to notify customers and end users of: ○ failures of components/systems ○ data breaches ○ data loss

Core skills

The employer set project (ESP) requires that students apply and contextualise core knowledge through the demonstration of the following core skills. Parameters have been provided for each skill in order to define what students must be able to demonstrate to fully satisfy the requirements of the ESP.

Core skill 1: Communicate information clearly to technical and non-technical stakeholders

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 3: Data • Route core element 6: Diversity and inclusion • Route core element 9: Planning • Route core element 12: Tools • Pathway core element 1: Careers within the digital support services sector • Pathway core element 2: Communication in digital support services

The student must be able to:

CS1. Communicate information clearly to a technical and non-technical audience:
• identify stakeholder requirements:
  ○ technical or non-technical terminology
  ○ formal or informal
  ○ digital level of knowledge
• identify key factors to determine scope of communication to meet stakeholder requirements:
  ○ required format
  ○ frequency of communications
  ○ content and context:
  ▪ design and layout
  ▪ level of detail
  ▪ digital inclusion
  ○ compliance with guidelines
• apply the identified requirements for the communications

The student must be able to:

• select and apply appropriate tools to communicate with stakeholders:
  ○ presentation tools
  ○ project management tools
  ○ collaborative communication tools
• record and document appropriate communications information:
  ○ summarise key points of communication
  ○ process and store data in compliance with relevant legislation and guidelines
(GEC1, GEC2, GEC3, GEC4, GEC6, GMC10, GDC1, GDC2, GDC3, GDC4, GDC5)

Core skill 2: Working with stakeholders to clarify and consider options to meet requirements

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 2: Culture • Route core element 3: Data • Route core element 9: Planning • Route core element 12: Tools • Pathway core element 2: Communication in digital support services

The student must be able to:

CS2. Work with stakeholders to clarify and consider options to meet requirements:
• identify scope of processes and expected outcomes:
  ○ collect data to clarify appropriate details
  ○ estimate budget and timescales
  ○ assess and calculate potential risk to meet requirements
  ○ assess cultural impacts to meet requirements
• analyse options to meet stakeholder requirements

The student must be able to:

• discuss with stakeholders to agree parameters based on analysis of options:
  ○ ask and respond to questions to clarify understanding
  ○ explain and present information using technical language correctly and coherently
  ○ encourage contributions from all stakeholders
  ○ summarise key points of discussion
• identify roles of stakeholders:
  ○ responsibilities
  ○ accountabilities
  ○ consulted
  ○ informed
• systematically organise and accurately record decisions and changes
• gather, process and store all information and data responsibly, in compliance with appropriate regulations and standards
(GEC1, GEC2, GEC3, GEC6, GMC2, GMC5, GMC10, GDC1, GDC5, GDC6)

Core skill 3: Apply a logical approach to solving problems, identifying and resolving faults, whilst recording progress and solutions to meet requirements

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 3: Data • Route core element 4: Digital analysis • Route core element 5: Digital environments • Route core element 7: Learning • Route core element 9: Planning • Route core element 11: Testing • Pathway core element 3: Fault analysis and problem resolution

The student must be able to:

CS3. Apply a logical approach to solving problems, identifying and resolving faults whilst recording progress and solutions:
• identify and investigate the scope of the problem
• decomposition of problem into component parts:
  o identify and analyse individual issues
• prioritisation of identified issues
• identify possible solutions
• plan, implement and test possible solutions
• apply appropriate solutions based on tested outcomes
• accurately record progress and outcomes:
  o use technical language correctly to aid understanding of outcomes
  o organise outcomes logically and coherently
• record and store data in compliance with relevant legislations and guidelines:
  o include the appropriate level of detail to meet requirements
(GEC1, GEC3, GMC5, GMC10, GDC1, GDC4)

Core skill 4: Ensure activity avoids risks to security

Route core underpinning knowledge
• Route core element 1: Business context • Route core element 8: Legislation • Route core element 9: Planning • Route core element 10: Security • Pathway core element 3: Fault analysis and problem resolution

The student must be able to:
CS4. Ensure activity avoids risks to security:

The student must be able to:

• identify and record potential risks:
  ○ threats
  ○ vulnerabilities
• assess probability and impact of risk
• calculate the severity and interpret the priority of risk, based on the probability and impact
• identify and apply appropriate risk mitigation controls and components
• record outcomes:
  ○ include the appropriate level of detail to meet requirements
• comply with relevant legislations and guidelines
(GEC3, GEC4, GMC6, GMC4, GDC1, GDC4, GDC5)

Occupational specialism: Digital Infrastructure

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The ‘K’ and ‘S’ indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data

Knowledge – What you need to teach

The student must understand:

K1.1 The role and types of preventative business control techniques in protecting the digital security of an organisation:

- role – proactive control that stops something happening
- preventative control techniques:
  - physical:
    - specialist locks (for example anti-picking)
    - barriers (for example fencing, bollards)
    - gates
    - cages
    - flood defence systems
    - temperature controls (for example air conditioning)
  - combined – managed access:
    - card readers
    - biometric
    - video/closed-circuit television (CCTV)
    - pin/passcodes
  - administrative, policies and procedures:
    - separation of duties and relevance of role-based access
  - technical – domains and security policies:

Knowledge – What you need to teach

- whitelisting
- blacklisting
- access control lists
- sandboxing
- device hardening
- certificate authority

K1.2 The role and types of detective business control techniques in protecting the digital security of an organisation:

- role – to identify an incident in progress or retrospectively
- detective control techniques:
  - physical:
    - CCTV
    - motion sensors
  - administrative, policies and procedures:
    - logs (for example logs of temperature in server room, error logs)
    - review/audit (for example people entering and leaving the facilities)

K1.3 The role and types of corrective business control techniques in protecting the digital security of an organisation:

- role – reactive measures to limit the extent of damage and reoccurrence
- corrective control techniques:
  - physical:
    - fire suppression (for example sprinklers, extinguishers)
    - gas suppression (for example inert and chemical gas systems)
  - administrative, policies and procedures:
    - standard operating procedure (for example actions taken when a fire is identified)

K1.4 The role and types of deterrent business control techniques in protecting the digital security of an organisation:

- role – pre-emptive measures to dissuade a course of action
- deterrent control techniques:
  - physical:
    - security guards

Knowledge – What you need to teach

- alarm systems
- visible surveillance systems

- administrative, policies and procedures:
  - standard operating procedure (for example setting alarm system, fire drill)
  - employment contracts stipulating codes of conduct
  - acceptable usage policies

K1.5 The role and types of directive business control techniques in protecting the digital security of an organisation:

- role – promotes a security-focused business culture
- directive control techniques:
  - physical:
    - signage
    - mandatory ID badge display (for example employees and visitors)
  - administrative, policies and procedures:
    - agreement types
    - general security policies and procedures
    - regular and compulsory staff training (for example human firewall training)

K1.6 The role and types of compensating business control techniques in protecting the digital security of an organisation:

- role – provides a safeguard against primary control failure
- compensating control techniques:
  - physical:
    - temperature controls (for example air conditioning)
  - administrative, policies and procedures:
    - role-based awareness training
    - standard operating procedures (for example environmental control monitoring)

K1.7 The role and implementation of a disaster recovery plan in protecting the digital security of an organisation:

- role – to recover and maintain service
- disaster recovery plan:
  - physical:

Knowledge – What you need to teach

- back-ups
- off-site alternative storage of servers

- administrative, policies and procedures of a disaster recovery plan (DRP) supported by an organisational business continuity plan (BCP):
  - ensuring all systems maintain functionality (for example arranging hardware)
  - ensuring users can access systems away from the main building site
  - deploying back-ups to maintain data integrity
  - ensuring digital changes continue to meet business needs
  - managing assets across the network and logging changes (for example tagging and logging laptops)
  - reporting infrastructure changes to management

K1.8 How a disaster recovery plan (DRP) works:

- define the scope of the plan:
  - data centre premises
  - organisational
  - departmental
  - individual
- gathering relevant information:
  - historic outage details
  - inventories of hardware, software, networks and data
  - contact information for any involved parties
- risk-assessing:
  - assets
  - threats
  - vulnerabilities
  - probability of occurrence
  - impact on business/data
- creating the plan:
  - identify the resources required for the DRP:
    - systems

Knowledge – What you need to teach

        - equipment
    - plan approval:
        - sign off by appropriate party
    - testing the plan:
        - identify scope
        - identify resources
        - determining frequency
        - implement test
        - review and document outcome
        - amend the plan based on review as required
    - continuous improvement:
        - internal and external auditing of plan

K1.9 The types of impacts that can occur within an organisation as a result of threats and vulnerabilities:

- danger to life – breaches in health and safety policies (for example injury and death)
- privacy – breaches of data (for example compromised confidential business data, identity theft)
- property and resources – damage to property and systems
- economic – financial loss or impairment
- reputation – damage to brand and business value
- legal – fines or prosecution

K1.10 The potential vulnerabilities in critical systems:

- unauthorised access to network infrastructure
- unauthorised physical access to network ports
- single point of failure
- system failure
- open port access:
    - USB (universal serial bus)
    - optical media:
        - compact disc (CD)
        - digital versatile disc (DVD)

Knowledge – What you need to teach

- wireless networks

K1.11 The impact of measures and procedures that are put in place to mitigate threats and vulnerabilities:

- measures:
  - recovery time objective (RTO)
  - recovery point objective (RPO)
  - mean time between failure (MTBF)
  - mean time to repair (MTTR)
- procedures:
  - standard operating procedure (SOP):
    - installation procedure
    - back-up procedure
    - set-up procedure
  - service level agreement (SLA):
    - system availability and uptime
    - response time and resolution timescales

K1.12 The process of risk management:

- process:
  - identification – identifying potential risks, threats or vulnerabilities
  - probability – likelihood of occurrence (for example high, medium, low)
  - impact – assess damage that can occur (for example asset value)
  - prioritisation – rank risks based on the analysis of probability and impact, ownership of risk
  - mitigation – reducing probability or impact of risk

K1.13 Approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – non-numeric:
    - determine severity using RAG rating:
      - red – high risk requiring immediate action
      - amber – moderate risk that needs to be observed closely
      - green – low risk with no immediate action required

Knowledge – What you need to teach

- quantitative – numeric:
  - analyse effects of risk (for example cost overrun, resource consumption)
- tools:
  - fault tree analysis
  - impact analysis
  - failure mode effect critical analysis
  - annualised loss expectancy (ALE)
  - Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)
  - strength, weakness, opportunity, threat (SWOT) analysis
  - risk register – risk is identified and recorded using a RAG rating
  - risk matrix – used to calculate the RAG rating for a risk

K1.14 Factors involved in threat assessment for the mitigation of threats and vulnerabilities:

- environmental:
  - extreme weather
  - natural disaster
  - animals (for example rodent in server room)
  - humidity
  - air quality
- manmade:
  - internal:
    - malicious or inadvertent activity from employees and contractors
  - external:
    - malware
    - hacking
    - social engineering
    - third-party organisations
    - terrorism
- technological:
  - technology failures and faults:

Knowledge – What you need to teach

- misconfigured devices
- disk failure/corruption
- component failure
- power issues
- network dropouts
- inaccessible systems
- virtual private network (VPN) not connecting
- unresponsive systems

- device failures and faults (for example laptops, desktops, servers):
  - hard disk failure
  - random access memory (RAM) failure
  - damaged peripherals
  - device incorrectly configured
  - additional card implementation (for example network interface card (NIC), graphics)
  - server back-up set-up
- system failures and faults:
  - firewall settings
  - software breakages/corruption
  - redundant array of independent disks (RAID) failure
- impact of technical change:
  - potential downtime
  - requirement for system or software upgrades
  - misconfigured systems

- political:
  - changes or amendments in legislation

K1.15 The purpose of risk assessment in a digital infrastructure context:

- purpose:
  - to identify and reduce risk by:

Knowledge – What you need to teach

- implementing Health and Safety Executive (HSE) guidelines to projects (for example installing a new uninterruptible power supply (UPS) system into a server room and identifying risks to the installers)
- investigating risks within the project environment (for example undertaking a PESTLE analysis)
- internal and external risk identification (for example implementing a supply chain assessment)
- quantification of impact on asset value (for example financial loss as a result of downtime)

K1.16 Types of risk response within a digital infrastructure context:

- types of response:
  - accept – the impact of the risk is deemed acceptable
  - avoid – change scope to avoid identified risk
  - mitigate – reduce the impact or probability of the identified risk
  - transfer – contractually outsource the risk to another party

K1.17 The process of penetration testing within digital infrastructure:

- the phases of penetration testing:
  - planning and reconnaissance (for example, scope, goals, gather intelligence)
  - scanning (for example, static and dynamic analysis)
  - gaining access (for example, back door, SQL injection)
  - maintaining access (for example, vulnerability used to gain in-depth access)
  - analysis and WAF configuration (for example, results collated into report, analysed and used to configure WAF settings)

K1.18 The considerations in the design of a risk mitigation strategy:

- risk response (for example accept, avoid, mitigate or transfer the risk)
- user profile (for example requirements, ability level)
- cost and benefit
- assign an owner of the risk
- escalation to appropriate authority within organisation
- planning contingencies
- monitoring and reviewing process

K1.19 The purpose of technical security controls as risk mitigation techniques and their applications to business risks within a digital infrastructure context:

Knowledge – What you need to teach

- purpose – to improve network security for users and systems
- technical security controls and their applications:
  - 5 cyber essentials controls:
    - boundary firewalls and internet gateways – restricting the flow of traffic in systems
    - secure configuration – ensuring user only has required functionality (for example removing unnecessary software, configuration to limit web access)
    - malware protection – maintaining up-to-date anti-malware software and regular scanning
    - patch management – maintaining system and software updates to current levels
    - access control – restricting access to a minimum based on user attributes (for example principle of least privilege, username and password management)
  - device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access
  - segmentation – network, systems, data, devices and services are split up to mitigate the potential impact of risks
  - hardware protection – using server and software solutions to protect hardware and data
  - multi-factor authentication – allowing 2 devices to authenticate against one system to confirm who and where the user is trying to access from
  - remote monitoring and management (RMM) (for example end user devices)
  - vulnerability scanning (for example port scanning, device scanning)

K1.20 The purpose and types of encryption as a risk mitigation technique and their applications:

- purpose – to store and transfer data securely using cryptography
- types of encryption and their applications:
  - asymmetric encryption – applied to send private data from one user to another (for example encrypted email systems)
  - symmetric encryption – applied to encrypt and decrypt a message using the same key (for example card payment systems)
  - data at rest encryption:
    - full disk encryption – applied to encrypt the contents of an entire hard drive using industry standard tool (for example Windows, macOS)
    - hardware security module (HSM) – safeguards digital keys to protect a device and its data from hacking
    - trusted platform module (TPM) – applied to store encryption keys specific to the host device
  - data in transit encryption:

Knowledge – What you need to teach

- secure sockets layer (SSL) – applied to create an encrypted link between a website and a browser using security keys for businesses to protect the data on their websites
- transport layer security (TLS) – applied to encrypt end-to-end communication between networks (for example in email, websites and instant messaging)

K1.21 The purpose, criteria and types of back-up involved in risk mitigation:

- purpose:
  - maintaining an up-to-date copy of data to enable future recovery and restoration (for example full disaster recovery or partial data loss)
- back-up criteria:
  - frequency (for example periodic back-ups)
  - source (for example files or data)
  - destination (for example internal, external)
  - storage (for example linear tape open (LTO), cloud, disk)
- types of back-up:
  - full
  - incremental
  - differential
  - mirror

K1.22 The relationship between organisational policies and procedures and risk mitigation:

- organisational digital use policy:
  - standard operating procedures for:
    - network usage and control (for example monitoring bandwidth, identifying bottlenecks)
    - internet usage (for example restricted access to sites, social media)
    - bring your own device (BYOD)
    - working from home (WFH) (for example DSE assessment)
    - periodic renewal of password
    - software usage (for example updating applications)
- health and safety policy for:
  - standard operating procedures:
    - lone working
    - manual handling/safe lifting (for example moving hardware)

Knowledge – What you need to teach

- working at height
- fire safety (for example staff training)
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013

- change procedure – approval and documentation of all changes
- auditing of policies and standard operating procedures – ensuring all actions are routinely examined (for example to ensure continued compliance)

K1.23 The purpose and application of legislation, industry standards and regulatory compliance, and industry best practice guidelines for the security of information systems within digital infrastructure.

Legislation:

- UK General Data Protection Regulation (UK GDPR):
  - purpose – standardises the way data is used, stored and transferred to protect privacy
  - applications within digital infrastructure:
    - article 1 – subject matter and objectives
    - article 2 – material scope
    - article 3 – territorial scope
    - article 4 – definitions
    - article 5 – principles relating to processing of personal data
    - article 6 – lawfulness of processing
    - article 7 – conditions for consent
- Data Protection Act (DPA) 2018:
  - purpose – implementation of UK GDPR to protect data and privacy
  - applications within digital infrastructure:
    - used fairly, lawfully and transparently
    - used for specified, explicit purposes
    - used in a way that is adequate, relevant and limited to only what is necessary
    - accurate and, where necessary, kept up-to-date
    - kept for no longer than is necessary
    - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- Computer Misuse Act 1990:

Knowledge – What you need to teach

- purpose – protects an individual's computer rights
- applications within digital infrastructure:
  - unauthorised access to computer materials (point 1 to 3)
  - unauthorised access with intent to commit or facilitate commission of further offences (point 1 to 5)
  - unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (point 1 to 6)

Industry standards and regulatory compliance:

- ISO 27001:
  - purpose – certifiable standard for information security management
  - applications within digital infrastructure:
    - UK GDPR/DPA 2018
    - information security
    - information management
    - penetration testing
    - risk assessments
- Payment Card Industry Data Security Standard (PCI DSS):
  - purpose – worldwide standard for protecting business card payments to reduce fraud
  - applications within digital infrastructure:
    - build and maintain a secure network
    - protect cardholder data
    - maintain a vulnerability management program
    - implement strong access control measures
    - regularly monitor and test networks
    - maintain an information security policy

Industry best practice guidelines:

- National Cyber Security Centre (NCSC) '10 Steps to Cyber Security':
  - purpose – inform organisations about key areas of security focus
  - applications within digital infrastructure:
    - user education and awareness

Knowledge – What you need to teach

        - home and mobile working
        - secure configuration
        - removable media controls
        - managing user privileges
        - incident management
        - monitoring
        - malware protection
        - network security
        - risk management regime
    - Open Web Application Security Project (OWASP):
        - purpose:
            - implement and review the usage of cyber security tools and resources
            - implement education and training into the general public and for industry experts
            - used as a networking platform
        - applications within digital infrastructure:
            - support users with online security
            - improve security of software solutions

K1.24 Principles of network security and their application to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data:

- the CIA triad – confidentiality, integrity and availability applied to develop security
- identification, authentication, authorisation and accountability (IAAA) – applied to prevent unauthorised access by implementing security policies to secure a network further:
    - applying directory services
    - security authentication process
    - using passwords and security implications
    - identification and protection of data
    - maintaining an up-to-date information asset register

K1.25 Methods of managing and controlling access to digital systems and their application within the design of network security architecture:

- authentication – restricts or allows access based on system verification of user
- firewalls – restricts or allows access to a defined set of services

Knowledge – What you need to teach

- intrusion detection system (IDS) – analyses and monitors network traffic for potential threats
- intrusion prevention system (IPS) – prevents access based on identified potential threats
- network access control (NAC) – restricts or allows access based on organisational policy enforcement on devices and users of network
- mandatory access control (MAC) – restricts or allows access based on a hierarchy of security levels
- discretionary access control (DAC) – restricts or allows access based on resource owner preference
- attribute-based access control (ABAC) – restricts or allows access based on attributes or characteristics
- role-based access control (RBAC) – restricts or allows access to resources based on the role of a user

K1.26 Physical and virtual methods of managing and securing network traffic and their application within the design of network security architecture:

- physical (for example server management, firewalls and cabling):
  - software defined networking (SDN):
    - transport layer security (TLS) (for example used in banking websites)
  - demilitarised zone (DMZ)
  - air gapping
- virtual:
  - virtual LAN (VLAN):
  - subnets:
  - virtual private network (VPN) (for example intranet, file systems, local network systems)
  - virtual routing and forwarding (VRF)
  - IP security (IPSec)
  - air gapping

K1.27 The principles and applications of cyber security for internet connected devices, systems and networks:

- the CIA (confidentiality, integrity and availability) triad – applied to assess the impact on security of systems (for example a data breach):
  - protection and prevention against a cyber attack through secure configuration of a network
  - limiting the network or system exposure to potential cyber attacks
  - detection of cyber attacks and effective logging/auditing to identify impacts

Knowledge – What you need to teach

- appropriate segregation of devices, networks and resources to reduce the impact of a cyber attack

K1.28 Techniques applied to ensure cyber security for internet connected devices, systems and networks:

- wireless security – WPA2 and use of end-to-end security implemented to monitor access to WiFi systems
- device security – password/authentication implemented to improve device security
- encryption
- virtualisation
- penetration testing
- malware protection
- anti-virus protection
- software updates and patches
- multi-factor authentication
- single logout (SLO)

K1.29 The importance of cyber security to organisations and society:

- organisations:
  - protection of:
    - all systems and devices
    - cloud services and their availability
    - company data and information (for example commercially sensitive information)
    - personnel data and data subjects (for example employee information, customer information)
  - password protection policies for users and systems
  - adherence to cyber security legislation to avoid financial, reputational and legal impacts
  - protection against cybercrime
- society:
  - protection of personal information to:
    - maintain privacy and security
    - protect from prejudices
    - ensure equal opportunities
    - prevent identity theft

Knowledge – What you need to teach

- individuals' rights protected under DPA 2018:
  - be informed about how data is being used
  - access personal data
  - have incorrect data updated
  - have data erased
  - stop or restrict the processing of data
  - data portability (for example allowing individuals to access and reuse their data for different purposes)
  - object to how data is processed in certain circumstances
- protection against cybercrime

K1.30 The fundamentals of network topologies and network referencing models and the application of cyber security principles:

- topologies:
  - bus
  - star
  - ring
  - token ring
  - mesh
  - hybrid
  - client-server
  - peer-to-peer
- network referencing models:
  - open systems interconnection (OSI) model:
    - application layer
    - presentation layer
    - session layer
    - transport layer
    - network layer
    - data link layer
    - physical layer

Knowledge – What you need to teach

- transmission control protocol/internet protocol (TCP/IP):
  - application layer
  - transport layer
  - network layer
  - network interface layer

- the minimum cyber security standards principles applied to network architecture:
  - identify – management of risks to the security of the network, users and devices:
    - assign cyber security lead
    - risk assessments for systems to identify severity of different possible security risks
    - documentation of configurations and responses to threats and vulnerabilities
  - protect – development and application of appropriate control measures to minimise potential security risks:
    - implementation of anti-virus software and firewall
    - reduce attack surface
    - use trusted and supported operating systems and applications
    - decommission of vulnerable and legacy systems where applicable
    - performance of regular security audits and vulnerability checks
    - data encryption at rest and during transmission
    - assign minimum access to users
    - provide appropriate cyber security training
  - detect – implementation of procedures and resources to identify security issues:
    - installation and application of security measures
    - review audit and event logs
    - network activity monitoring
  - respond – reaction to security issues:
    - contain and minimise the impacts of a security issue
  - recover – restoration of affected systems and resources:
    - back-ups and maintenance plans to recover systems and data
    - continuous improvement review

Knowledge – What you need to teach

K1.31 Common vulnerabilities to networks, systems and devices and the application of cyber security controls:

- missing patches, firmware and security updates:
  - application of cyber security controls:
    - patch manager software
    - tracking network traffic
    - test groups/devices to test security
- password vulnerabilities (for example missing, weak or default passwords, no password lockout allowing brute force or dictionary attacks):
  - application of cyber security controls:
    - minimum password requirements in line with up-to-date NCSC guidance (for example length, special character)
    - password reset policy
- insecure basic input-output system (BIOS)/unified extensible firmware interface (UEFI) configuration:
  - application of cyber security controls:
    - review BIOS/UEFI settings
    - update BIOS
- misconfiguration of permissions and privileges:
  - application of cyber security controls:
    - testing permissions and access rights to systems
    - scheduled auditing of permissions and privileges (for example remove access of terminated staff)
- unsecure systems due to lack of protection software:
  - application of cyber security controls:
    - protecting against malware (for example virus, worm, trojan, ransomware)
    - update security software
    - monitoring security software
    - buffer overflow
- insecure disposal of data and devices:
  - application of cyber security controls:
    - compliance with Waste Electrical and Electronic Equipment (WEEE) Directive 2013

Knowledge – What you need to teach

        - checking and wiping all data devices
- inadequate back-up management:
    - application of cyber security controls:
        - back-up frequency
        - application of appropriate types of back-up
- dynamic host configuration protocol (DHCP) spoofing:
    - application of cyber security controls:
        - using DHCP snooping
- VLAN attacks and VLAN hopping:
    - application of cyber security controls:
        - implementation testing of the VLAN
        - scheduled testing and monitoring of network
- misconfigured firewalls:
    - application of cyber security controls:
        - testing firewall
        - scheduled monitoring and updates
- exposed services and ports – allows network attacks (for example a user connecting their device to an ethernet port):
    - application of cyber security controls:
        - physical security controls
        - monitoring network traffic
- misconfigured access control lists (ACLs):
    - application of cyber security controls:
        - monitor and review ACLs
- ineffective network topology design (for example inadequate placement of firewalls and DMZ):
    - application of cyber security controls:
        - review of network topology design prior to implementation
        - implementation testing
- unprotected physical devices:
    - application of cyber security controls:

Knowledge – What you need to teach
▪ install correct software

Skills – What you need to teach

The student must be able to:

S1.1 Apply and maintain procedures and security controls in the installation, configuration and support of physical and virtual infrastructure to ensure confidentiality, integrity and availability:

- set up a domain services environment with security controls (for example group policies, minimum password requirements)
- set up and deploy a certificate authority (for example server deployment)
- implement security controls in a business environment in line with NCSC cyber essentials:
  - boundary firewalls
  - secure configuration (for example enabling multi-factor authentication)
  - access control
  - malware protection
  - patch management
- configure and apply appropriate access control methods to physical or virtual networks (for example authentication, MAC, DAC, ABAC, RBAC)
- manage documents and data accurately in accordance with data protection legislation

(GEC5, GDC1, GDC5, GDC6)

S1.2 Apply and monitor appropriate business control techniques and policies and procedures to ensure personal, physical and environmental security:

- review the identified risk:
  - gather information from system and users
- select, apply and monitor appropriate business control techniques:
  - preventative
  - detective
  - corrective
  - deterrent
  - directive
  - compensating
  - recovery
- comply with relevant regulatory and organisational policies and procedures

(GDC3)

S1.3 Explain the importance of organisational and departmental policies and procedures in respect of adherence to security:

Skills – What you need to teach

- explain the purpose and application of each policy and procedure, summarising key information and using appropriate technical terms:
  - digital use policy
  - health and safety policy
- explain the potential impact on security if policies and procedures are not adhered to (for example danger to life, privacy)

(GEC5, GDC5)

S1.4 Install and configure software for network and end user devices (for example servers, desktop computers) to identify and mitigate vulnerabilities:

- install and configure software to secure the network:
  - vulnerability scanning software (for example port scanning software, device scanning software)
  - anti-malware software
  - firewall software
- apply device hardening to remove unnecessary software
- check installation and configuration on end user devices

(GEC4, GDC1, GDC6)

S1.5 Conduct a security risk assessment in line with the risk management process for a system (for example a device connected to a local area network LAN):

- assess the system and identify components
- apply the risk management process:
  - identify possible risks within the system
  - calculate the probability and impact of the identified risk
  - analyse and prioritise based on level of risk to system
- record all relevant findings and actions accurately and concisely using appropriate technical terms

(GEC4, GMC6, GDC4)

S1.6 Demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a digital infrastructure context:

- identify, gather and systematically organise information on incidents in preparation for analysis
- process and analyse trends in incident data to identify underlying risks
- identify user profile (for example requirements, ability level)

Skills – What you need to teach

• identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices (for example installing RMM software, device hardening)
• monitor and review as part of a continuous improvement process:
  ○ assign an owner of the risk
  ○ plan contingencies
  ○ update devices with current security software
  ○ interpret the outputs of penetration testing
• record all relevant findings and actions accurately and concisely using appropriate technical terms
(GEC4, GMC5, GDC4)

Performance outcome 2: Explain, install, configure, test and manage both physical and virtual infrastructure

Knowledge – What you need to teach

The student must understand:

K2.1 The principles of network and infrastructure design:

- resilience:
  - high availability (HA) – primary and secondary configurations of systems to provide redundancy
  - clustering – provides redundancy and scalability
  - load balancing – directs network traffic based on load
  - segmentation – network, systems, data, devices and services are split up to mitigate the potential impact of risks
- quality of service (QoS) – used to guarantee a specific network service
- number systems – applied for subnetting and IP addressing:
  - binary
  - hexadecimal
  - decimal
  - octal

K2.2 The principles of the transmission of digital information over copper cable, fibre cable and wireless networks and systems:

- signal type:
  - electrical-based
  - light-based
  - wireless
- security:
  - tampering
  - signal loss
- segregation from electrical cables:
  - susceptibility to interference:
    - types of interference (for example electromagnetic impact on signal, static, crosstalk)
    - mitigation techniques (for example shielding, run cables in parallel)
    - adhering to industry standards

Knowledge – What you need to teach

- BS EN 50174

- wireless bands and channels:
  - 2.4GHZ:
    - 802.11b
    - 802.11g
    - 802.11n
    - 802.11ax
  - 5GHZ:
    - 802.11ac
    - 802.11n
    - 802.11ax
- internet protocol version 4 (IPv4) network and subnets:
  - addressing schemes
  - subnetting
  - subnet masks
- internet protocol version 6 (IPv6)):
  - IPv6 address types

K2.3 The elements of infrastructure and associated technologies:

- network devices:
  - firewalls (for example next generation firewall (NGFW))/unified threat management (UTM) appliances)
  - routers
  - switches
  - hubs
  - bridges
  - wireless/WiFi access points (APs)
  - wireless range extenders:
  - modems
  - media converters
- end user devices (EUDs):

Knowledge – What you need to teach

- desktops and laptops
- mobile devices (for example smartphone, tablet)
- smart devices (for example wearable technology, smart speakers)

- storage devices and systems:
  - hard disk drive (HDD)
  - solid state drive (SSD)
  - removable media (for example USB flash drive, external hard drive)
  - network-attached storage (NAS)
  - storage area network (SAN)
  - block storage
  - object storage
  - redundant array of independent disks (RAID):
    - RAID 0 – striping
    - RAID 1 – mirroring
    - RAID 5 – parity across drives
    - RAID 10 – mirroring and striping
- wired and wireless technologies:
  - unshielded twisted pair (UTP) cable:
    - straight-through
    - crossover
    - EIA/TIA-568A layout
    - EIA/TIA-568B layout
  - RJ11 connectors
  - 8P8C/RJ45 connectors
  - copper cables (for example cat 5e, cat6)
  - fibre-optic cables
  - the point-to-point protocol (PPP)
  - SDN
  - WiFi protected access (WPA) 1, 2, and 3
- antennas:

Knowledge – What you need to teach
○ omni-directional ○ directional ○ patch ○ yagi ○ dipole • cloud services: ○ IaaS ○ PaaS ○ SaaS ○ cloud storage • test equipment: ○ test plan ○ testing kit: ▪ tone generator and probe ▪ cable tester ▪ tracing kit • support scripting (for example automation and administration) • network monitoring and logging. • capacity management (for example monitoring server load) **K2.4 The requirements of static prevention when working with electrostatic-sensitive equipment:** • mobility awareness (for example limiting movement to avoid electrostatic discharge (ESD)) • temperature/humidity checks (for example increased humidity resulting in increased static electricity) • application of static prevention equipment (for example anti-static wrist strap) **K2.5 Health and safety legislation and regulations in the workplace and their application in a digital infrastructure context:** • Health and Safety at Work etc Act 1974 (for example providing appropriate PPE, employer safeguarding) • Manual Handling Operations Regulations 1992 (for example moving hardware) • Health and Safety (Display Screen Equipment) Regulations 1999 (as amended in 2002) (for example reducing screen time, correctly configured workspaces)

Knowledge – What you need to teach

- Control of Substances Hazardous to Health (COSHH) Regulations 2002 (for example printer maintenance)
- Control of Major Accident Hazards (COMAH) Regulations 2015 (for example earthing)
- Waste Electrical and Electronic Equipment (WEEE) Directive 2013 (for example removal or disposal of hardware or network components)

K2.6 The advantages and limitations of physical servers:

- advantages:
  - full access to server resources required for business-critical operations
  - fully customisable and configurable to business requirements
- limitations:
  - high purchase and running costs
  - increased time allocation for maintenance
  - storage cannot be scaled as easily as other server types
  - requires physical space

K2.7 The advantages and limitations of self-hosted and cloud-hosted virtual servers:

- self-hosted server (virtual server on a physical host):
  - advantages:
    - lower expertise required to set up
    - greater control of costs
    - scaling can be applied
    - high availability (HA)/clustering
  - limitations:
    - high upfront cost
    - high cost for resilience
- cloud-hosted virtual server (for example Microsoft Azure, Amazon Web Services):
  - advantages:
    - scaling can be applied easily
    - built in redundancy
    - third-party support provided
  - limitations:
    - high subscription cost

Knowledge – What you need to teach

- complex initial set-up

K2.8 The advantages and limitation of containers:

- advantages:
  - require fewer system resources
  - easily deployable due to portability
  - applications run more consistently and efficiently
  - low operating and development costs
- limitations:
  - less secure if not configured correctly
  - less flexibility on operating systems
  - higher level of expertise required to set up and configure

K2.9 The types, benefits, similarities and differences of operating systems (OSs) and their application within digital infrastructure:

- types of operating systems:
  - end user/desktop (for example Windows, macOS) – applied to desktop PCs and laptops
  - mobile (for example Android, iOS) – applied to tablets and mobile devices
  - server (for example Linux, Windows Server) – applied to client-server environments
- benefits of operating systems:
  - improved usability
  - no required knowledge of machine language from user
  - increased security of data
- similarities across operating systems:
  - provides user interface
  - allows personalisation
  - manages resources
  - provides platform for installation of applications
- differences between operating systems:
  - specific features aligned to purpose (for example personal use, supporting client-server architecture)
  - provides different levels of user experience (UX) and user interface (UI)
  - supports varying types of functionality (for example touchscreen, wireless charging)

Knowledge – What you need to teach

K2.10 Service functions and their application within a client-server network environment:

- active directory domain services (AD DS):
  - active directory – provides functionality to centrally manage and organise user and device accounts, security groups and distribution lists, contained in organisational units (OUs)
  - group policy – provides functionality to create group policy objects (GPOs) which can be applied to OUs. GPOs can be applied to deploy settings and files to users' profiles and devices, based on their OU
- dynamic host configuration protocol (DHCP) – to assign IP addresses to network client devices
- lightweight directory access protocol (LDAP) – used for directory services authentication
- domain name system (DNS) – for the translation of hostnames to IP addresses
- file server and distributed file system (DFS) – to provide shared disk access
- print server – to provide shared printer access
- web, proxy and cache servers – to provide efficient internet/web access, security and filtering
- mail servers – to handle the sending and receiving of emails to/from client mailboxes
- application servers – to provide access to network-based applications
- database servers – to provide backend shared databases
- security utilities (for example anti-virus) – to protect data or systems against loss or attack

K2.11 Methods of remote access and how they protect data:

- virtual private network (VPN) – network is private and the connection is encrypted to prevent any unauthorised access
- remote desktop protocol (RDP) (for example proprietary RDP software) – data processing occurs on the machine being accessed, no data is transferred to the client machine
- lights-out management (LOM) – the server can be remotely managed and many tasks carried out to address problems or unauthorised access
- secure shell (SSH) – the connection is secure, only the 2 hosts can access the data

K2.12 The considerations involved in setting up a simple VPN to enable secure remote access:

- configuration of the VPN server:
  - enabling the VPN service
  - configuring IP address and DNS hostnames of the VPN interface
  - managing user access including authentication and permissions
- configuration of the client device:
  - creating the connection

Knowledge – What you need to teach

- setting the destination IP address and fully qualified domain name (FQDN)
- setting permissions and conditions

K2.13 The principles of IT service management (ITSM):

- the co-creation of value through service relationships
- the delivery of great experience to customers
- considering the broader scope and potential impact of changes
- working across departments to learn how others use the systems

K2.14 The Information Technology Infrastructure Library (ITIL®) framework and how this is applied in a digital infrastructure context:

- service strategy – aligned to business objectives to ensure that the service is fit for purpose and fit for use
- service design – design of services and all supporting elements for introduction into the live environment, ensuring that people, processes, products and partners are all considered
- service transition – building and deploying services and ensuring that any changes are managed in a coordinated way
- service operation – fulfilling requests, resolving failures, fixing problems and carrying out routine operational tasks
- continual service improvement – continually improving the effectiveness and efficiency of IT processes and services

K2.15 The principles of disaster recovery plans (DRPs) and business continuity plans (BCPs):

- key principles:
  - identify:
    - risk
    - operational critical systems
    - requirements (for example resources)
  - analyse:
    - business impact (for example impact on departments, customers, suppliers)
    - maximum downtime
  - design:
    - plan components
  - implement:
    - communication plan

Knowledge – What you need to teach

- measure:
  - test
  - compliance (for example with relevant legislation, policies and procedures)
  - review and maintain

K2.16 The different purpose of DRPs and BCPs in the context of digital infrastructure:

- BCP – planning and managing business continuity during a disruptive event:
  - alternative business premises
  - adaptive policies and processes
  - application of alternative technologies
- DRP – restoring normal business operations following a disaster (for example flood):
  - restoring functionality or access
  - replacement of infrastructure resources

K2.17 The stages within a solution lifecycle (SLC):

- stages:
  - discover:
    - business requirements
    - project definition and planning
    - conceptual design
    - feasibility and viability
  - plan, design and develop:
    - detailed design and planning
    - proof of concept and prototyping
    - compliance with organisational policies and standards
    - utilisation of existing architecture and resources
    - development
    - integration
  - testing and quality assurance:
    - functional testing to ensure the product or service meets the agreed deliverables
    - performance testing
  - pre-production:

Knowledge – What you need to teach

        - sandboxed testing in a development environment
        - sign-off and authorisation to deploy
    - deployment:
        - release into the live/production environment
        - staged release plan for significant or high impact changes/updates
    - monitor and evaluate ongoing performance:
        - optimisation through continuous improvement in line with agreed change management processes
    - decommission
    - migrate to new solution

K2.18 The principles, aims and benefits of a DevOps approach:

- DevOps principles:
    - continuous integration
    - continuous delivery (for example deployment)
    - microservices
    - infrastructure as code
    - communication and collaboration
    - automated testing
    - adapt and scale
    - monitoring and logging
- aims:
    - to deliver systems, applications or services in an agile way
    - to build, test and release changes
- benefits:
    - rapid delivery of solutions (for example through automation)
    - increased productivity
    - improved processes across teams
    - scalability
    - reduced errors

K2.19 The principles of solution architecture:

Knowledge – What you need to teach

- the importance of reuse
- the importance of documentation
- solution architecture as applied to hardware
- adherence to architecture frameworks (for example The Open Group Architecture Framework (TOGAF))
- alignment to enterprise architecture
- architecture description:
  - system
  - view
  - viewpoint
  - concern
  - stakeholder

K2.20 The concepts of virtualisation and the areas of application within digital infrastructure:

- concepts:
  - the creation of many virtual resources from one physical resource (for example partitioning)
  - the creation of one virtual resource from one or more physical resources
  - isolation
  - encapsulation
  - hardware independence
- areas of application within digital infrastructure:
  - network virtualisation
  - server virtualisation
  - desktop virtualisation
  - operating system virtualisation
  - data virtualisation

Skills – What you need to teach

The student must be able to:

S2.1 Explain the fundamentals of network infrastructure:

Skills – What you need to teach

- identify and explain the purpose and application of network infrastructure
- summarise and explain, using correct technical language, the benefits of network infrastructure within an organisation
- identify and explain the application of protocols and ports

(GEC1, GEC4)

S2.2 Assess workplace risk in regards to electrostatic discharge (ESD):

- apply the risk management process:
  - identify:
    - possible risks
    - effect of actions on themselves and others
  - calculate the probability and impact of the identified risk
  - prioritise based on level of risk
- record and logically organise all relevant findings in the appropriate format
- apply appropriate ESD protection devices when working with hardware
- comply with all relevant health and safety standards and regulations
- record and store all documents in compliance with appropriate legislation and regulations

(GEC1, GEC3, GMC2, GMC6, GMC10, GDC5)

S2.3 Install, configure and test physical and virtual networks:

- install and configure component parts of physical and virtual networks:
  - server:
    - types (for example physical, virtual)
    - operating systems (for example Windows, Linux)
    - applications:
      - database (for example storage)
      - security utilities (for example anti-virus)
  - network infrastructure appropriate devices
  - firewall
  - load balancer
  - end user devices (for example desktop PC, laptop, smartphone)
  - network-based services (for example DNS, DHCP)
- select and apply appropriate network ports and protocols

Skills – What you need to teach

- implement appropriate scripting
- apply appropriate back-up policies and procedures
- implement testing to monitor quality of network:
  - functionality
  - performance
- record all test results to inform network improvements

(GDC1, GDC6)

S2.4 Maintain the effective functioning of physical or virtual networks:

- maintain component parts of physical and virtual networks:
  - server:
    - types (for examples physical, virtual)
    - operating systems
    - applications:
      - databases
      - security utilities
  - firewall
  - load balancer
  - network infrastructure devices
  - network-based services:
    - DNS
    - DHCP
- review and optimise performance:
  - performance monitoring and logging systems (for example email alerts)
  - capacity management system (for example disk monitoring)
  - software and hardware utilisation
- apply automation via scripting

(GDC1, GDC6)

S2.5 Make and test a unshielded twisted pair (UTP) cable to required national and international standards:

- determine purpose of cable:
  - calculate required length

Skills – What you need to teach

- make:
  - straight-through cable
  - crossover cable
- select and apply appropriate equipment (for example 8P8C/RJ45 connectors, crimper, wire cutters)
- test in compliance with applied TIA/EIA standards

(GMC2)

S2.6 Demonstrate continuous improvement by maintaining the effective functioning of a range of hardware solutions (for example contemporary, legacy) and network in response to change:

- identify and assess the change:
  - identify the hardware affected by change
  - assess the current performance of the network
- apply the appropriate stages of a solution lifecycle to respond to change:
  - assess the performance of the network after the response
- process, analyse and review outcome data
- record and logically organise all relevant findings and actions accurately and concisely using appropriate technical terms to inform future policies and procedures:
  - summarise key information

(GEC1, GEC2, GEC4, GDC4)

S2.7 Demonstrate the ability to apply all stages of a solution lifecycle in a digital infrastructure context:

- apply the stages of solution lifecycle in a safe and responsible manner:
  - discover
  - plan, design and develop
  - test and quality assurance
  - pre-production
  - deployment
  - monitor and evaluate ongoing performance
  - decommission
  - migrate to new solution
- record and document decisions, actions and outcomes for each stage of the solution lifecycle

(GMC2, GMC3)

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach

The student must understand:

K3.1 Types of sources of knowledge that can be applied within digital infrastructure:

- academic publications (for example textbooks, research journals and periodicals)
- supplier literature (for example handbooks or online articles for specific devices, computers or laptops)
- search engines (for example Google, Bing)
- websites (for example wikis, forums, Stack Overflow, manufacturers' websites)
- social media (for example company profiles on Twitter, Facebook and LinkedIn)
- blogs (for example reviews of new technologies, opinions on topical issues in the digital sector)
- vlogs (for example demonstrations, tutorials on digital technologies)
- professional networks (for example digital transformation networking events/conferences)
- e-learning (for example massive open online courses (MOOCs), recognised vendor qualifications, Cisco)
- peers (for example colleagues, network contacts, other industry professionals)

K3.2 The factors of reliability and validity to be applied to legitimise the use of sources of knowledge:

- industry-certified accreditation (for example Cisco certified network associate (CCNA1), Microsoft technology associate (MTA), network fundamentals)
- appropriateness
- evidence-based:
  - citations
- relevant context
- credibility of author:
  - affiliated to specific bodies (for example government, industry regulators)
  - reputation
  - experience (for example relevant qualification in subject)
- target audience – produced with specific audience requirements taken into consideration (for example use of technical/non-technical terminology)
- publication:
  - version (for example use of the current version)

Knowledge – What you need to teach

- date of publication (for example if the content is outdated)

K3.3 The factors of bias:

- types of conscious and unconscious bias:
  - author/propriety bias – unweighted opinions of the author or owner
  - confirmation bias – sources support a predetermined assumption
  - selection bias – selection of sources that meets specific criteria
  - cultural bias – implicit assumptions based on societal norms
- indicators of bias within sources:
  - partiality
  - prejudice
  - omission
- bias reduction:
  - based on fact/evidence
  - inclusive approach
  - full representation of demographics:
  - objectivity

K3.4 Process of critical thinking and the application of evaluation techniques and tools:

- process of critical thinking:
  - identification of relevant information:
    - different arguments, views and opinions
  - analysis of identified information:
    - identify types of bias and objectivity
    - understand links between information and data
  - selection of relevant evaluation techniques and tools
  - evaluation of findings and drawing of conclusions
  - recording of conclusions
- evaluation techniques:
  - formative evaluation
  - summative evaluation
  - qualitative (for example interviews, observations, workshops)

Knowledge – What you need to teach

- quantitative (for example experiments, surveys, statistical analysis)
- benchmarking
- corroboration:
  - cross-referencing
- triangulation

- evaluation tools:
  - gap analysis
  - KPI analysis
  - score cards
  - observation reports
  - user diaries
  - scenario mapping
  - self-assessment frameworks
  - maturity assessments

K3.5 Methods of communication and sharing knowledge and their application within a digital infrastructure context:

- integrated and standalone IT service management tools:
  - incident and problem management systems
  - change management systems
- knowledge bases and knowledge management systems
- wikis and shared documents
- shared digital workspaces
- telephone
- instant messaging
- email
- video conferencing
- digital signage
- social media:
  - organisational
  - public

Knowledge – What you need to teach

- personal
- blogs
- community forums
- project management tools (from example issue logs, Gantt charts, Kanban boards, burndown charts)
- policy, process and procedure documents

Skills – What you need to teach

The student must be able to:

S3.1 Identify sources of knowledge and apply factors that legitimise their use to meet requirements in a digital infrastructure context:

- identify and clarify the parameters of the requirements
- identify appropriate sources of knowledge (up to 3) (for example search engines, blogs)
- apply the factors of reliability and validity to identified sources (for example authority, date of publication)
- assess and review potential bias of sources
- assess and review the identified sources' appropriateness to meet the requirements

(GEC4, GDC1)

S3.2 Search for information to support a topic or scenarios within digital infrastructure and corroborate information across multiple sources:

- identify and clarify the parameters of the search (for example explore the future of the digital economy, identify trends in big data)
- identify the sources of data that contain the required information
- safely and securely search sources for the information required
- corroborate sources by applying cross-referencing across multiple sources
- apply reliability and validity factors
- assess and review potential bias of sources

(GEC4, GDC5)

S3.3 Select and apply techniques and tools to support evaluation in a digital infrastructure context:

- identify and clarify the parameters of the evaluation
- select appropriate techniques and tools to support the evaluation

Skills – What you need to teach

- apply the selected techniques and use the appropriate tools to support the evaluation
- record the findings of the evaluation for the requirement

(GEC4, GDC2)

S3.4 Compare options of sources and rationalise the actions taken to ensure the reliability and validity of sources:

- identify the sources for comparison
- apply the relevant reliability and validity factors to the sources
- compare the outcomes of the validity and reliability actions
- explain and recommend the choice of action to ensure the sources are reliable and valid, using appropriate technical terms

(GEC1, GEC3, GEC5, GMC5, GDC3)

S3.5 Identify and understand bias when using sources of knowledge in a specific digital infrastructure context:

- identify the types of bias (for example confirmation, unconscious)
- identify the indicators of bias within the source
- explain clearly and concisely how bias has been created within the source
- explain clearly and concisely how bias can be avoided within sources

(GEC1, GEC3, GEC5, GMC6, GDC3)

S3.6 Demonstrate critical thinking within a digital infrastructure context:

- apply the process of critical thinking to meet requirements:
  - identify relevant information
  - analyse the information
  - select and apply appropriate evaluation techniques and tools
  - evaluate findings
  - logically organise and record conclusions

(GEC1, GEC3, GMC5, GMC6, GMC8, GDC3, GDC4)

Occupational specialism: Network Cabling

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The ‘K’ and ‘S’ indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install and test cabling in line with technical and security requirements
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data

Knowledge – What you need to teach

The student must understand:

K1.1 Types of preventative business control techniques used in protecting the digital security of an organisation:

- preventative control techniques:
  - physical:
    - specialist locks (anti-picking)
    - barrier (for example fencing bollards)
    - gates
    - cages
    - lock/key or equivalent
  - combined – managed access:
    - card readers
    - biometric
    - video
    - pin/passcodes
  - administrative, policies and procedures:
    - separation of duties and relevance of role-based access
  - technical – domains and security policies:
    - whitelisting
    - blacklisting

Knowledge – What you need to teach

- access control lists
- sandboxing
- device hardening
- certificate authority

K1.2 Types of detective business control techniques in protecting the digital security of an organisation:

- detective control techniques:
  - physical:
    - CCTV
    - motion sensors
  - administrative, policies and procedures:
    - logs (for example error logs)
    - review/audit (for example people entering and leaving the facilities)

K1.3 Types of corrective business control techniques in protecting the digital security of an organisation:

- corrective control techniques:
  - physical:
    - fire suppression (for example sprinklers, extinguishers)
    - gas suppression systems (for example inert and chemical gas systems)
  - administrative, policies and procedures:
    - standard operating procedure (for example actions taken when a fire is identified)

K1.4 Types of deterrent business control techniques in protecting the digital security of an organisation:

- deterrent control techniques:
  - physical:
    - security guards
    - alarm systems
    - visible surveillance systems
  - administrative, policies and procedures:
    - standard operating procedure (for example setting alarm system, fire drill)
    - employment contracts stipulating codes of conduct

Knowledge – What you need to teach

- acceptable usage policies

K1.5 Types of directive business control techniques in protecting the digital security of an organisation:

- directive control techniques:
  - physical:
    - signage
    - mandatory ID badge display (employees and visitors)
  - administrative, policies and procedures:
    - agreement types
    - general security policies and procedures
    - regular and compulsory staff training (for example human firewall training)

K1.6 Types of compensating business control techniques in protecting the digital security of an organisation:

- compensating control techniques:
  - physical:
    - temperature controls (for example air conditioning)
  - administrative, policies and procedures:
    - role-based awareness training
    - standard operating procedures (for example environmental control monitoring)

K1.7 Components of a disaster recovery plan in protecting the digital security of an organisation:

- disaster recovery plan (DRP):
  - physical:
    - back-ups
    - off-site alternate storage
  - administrative, policies and procedures of a DRP supported by an organisational business continuity plan (BCP):
    - ensuring all systems maintain functionality (for example arranging hardware)
    - ensuring users can access systems away from the main building site
    - deploying back-ups to maintain data integrity
    - ensuring digital changes continue to meet business needs

Knowledge – What you need to teach

- managing assets across the network and logging changes (for example tagging and logging laptops)
- reporting infrastructure changes to management

K1.8 Types of impacts that can occur within an organisation as a result of threats and vulnerabilities:

- danger to life – breaches in health and safety policies (for example injury and death)
- privacy – breaches of data (for example compromised confidential business data, identity theft)
- property and resources – damage to property and systems
- economic – financial loss or impairment
- reputation – damage to brand and business value
- legal – fines or prosecution

K1.9 Potential vulnerabilities in critical systems:

- unauthorised access to network infrastructure
- unauthorised physical access to network ports
- single point of failure
- open port access:
  - universal serial bus (USB)
  - optical media:
    - compact disc (CD)
    - digital versatile disc (DVD)
- network ports
- wireless networks

K1.10 The impact of measures and procedures that are put in place to mitigate threats and vulnerabilities:

- measures:
  - recovery time objective (RTO)
  - recovery point objective (RPO)
  - mean time between failure (MTBF)
  - mean time to repair (MTTR)
- procedures:
  - standard operating procedure (SOP):
    - installation procedure

Knowledge – What you need to teach

- back-up procedure
- set-up procedure

- service level agreement (SLA):
  - system availability and uptime
  - response time and resolution timescales

K1.11 The process of risk management:

- process:
  - identification – identifying potential risks, threats or vulnerabilities
  - probability – likelihood of occurrence (for example high, medium, low)
  - impact – assess damage that can occur (for example asset value)
  - prioritisation – rank risks based on the analysis of probability and impact, ownership of risk
  - mitigation – reducing probability or impact of risk

K1.12 Approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – non-numeric:
    - determine severity using RAG rating:
      - red – high risk requiring immediate action
      - amber – moderate risk that needs to be observed closely
      - green – low risk with no immediate action required
  - quantitative – numeric:
    - analyse effects of risk (for example cost overrun, resource consumption)
- tools:
  - fault tree analysis
  - impact analysis
  - failure mode effect critical analysis
  - annualised loss expectancy (ALE)
  - Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)
  - strength, weakness, opportunity, threat (SWOT) analysis
  - risk register – risk is identified and recorded using a RAG rating

Knowledge – What you need to teach

- risk matrix - used to calculate the RAG rating for a risk

K1.13 Factors involved in threat assessment for the mitigation of threats and vulnerabilities:

- environmental:
  - extreme weather
  - natural disaster
  - animals (for example rodent chewing cables)
  - humidity
  - air quality
- manmade:
  - internal:
    - malicious or inadvertent activity from employees and contractors
  - external:
    - malware
    - hacking
    - social engineering
    - third-party organisations
    - terrorism
- technological:
  - technology failures and faults (for example WiFi dropouts, inaccessible systems)
  - device failure and faults (for example firewall setting, interference of signal)
  - impact of technical change (for example system upgrade, software upgrade)
- political:
  - changes to legislation

K1.14 The purpose of risk assessment in a network cabling context:

- purpose:
  - to identify and reduce risk by:
    - implementing Health and Safety Executive (HSE) guidelines to projects (for example installing a new uninterruptible power supply (UPS) system into a server room and identifying risks to the installers)
    - investigating risks within the project environment (for example undertaking a PESTLE analysis)

Knowledge – What you need to teach

- internal and external risk identification (for example implementing a supply chain assessment)
- quantification of impact on asset value (for example financial loss as a result of downtime)

K1.15 Types of risk response within a network cabling context:

- types of response:
  - accept – the impact of the risk is deemed acceptable (for example low impact, low probability)
  - avoid – change scope to avoid identified risk
  - mitigate – reduce the impact or probability of the identified risk
  - transfer – contractually outsource the risk to another party

K1.16 The process of penetration testing within network cabling:

- the phases of penetration testing:
  - planning and reconnaissance (for example scope, goals, gather intelligence)
  - scanning (for example static and dynamic analysis)
  - gaining access (for example back door, SQL injection)
  - maintaining access (for example vulnerability used to gain in-depth access)
  - analysis and web application firewall (WAF) configuration (for example, results collated into report, analysed and used to configure WAF settings)

K1.17 The considerations in the design of a risk mitigation strategy:

- risk response (for example accept, avoid, mitigate or transfer the risk)
- user profile (for example requirements, ability level)
- cost and benefit
- assign an owner of the risk
- escalation to appropriate authority within organisation
- planning contingencies
- monitoring and reviewing process

K1.18 The purpose of technical security controls as risk mitigation techniques and their applications to business risks:

- purpose – to improve network security for users and systems
- technical security controls and their applications:
  - 5 cyber essentials controls:
    - boundary firewalls and internet gateways – restricting the flow of traffic in systems

Knowledge – What you need to teach

- secure configuration – ensuring user only has required functionality (for example removing unnecessary software, configuration to limit web access)
- malware protection – maintaining up-to-date anti-malware software and regular scanning
- patch management – maintaining system and software updates to current levels
- access control – restricting access to a minimum based on user attributes (for example principle of least privilege, username and password management)

- device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access
- remote monitoring and management (RMM) (for example end user devices)
- anti-virus software – protecting against attacks from established threats

K1.19 The purpose and types of encryption as a risk mitigation technique and their applications:

- purpose – to store and transfer data securely using cryptography
- types of encryption and their applications:
  - asymmetric encryption – applied to sending private data between 2 users (for example encrypted email systems)
  - symmetric encryption – applied to sending private data between 2 users using the same key (for example card payment systems)
  - data at rest encryption:
    - full disk encryption – applied to encrypt the contents of an entire hard drive using industry standard tool (for example Windows, macOS)
    - hardware security module (HSM) – safeguards digital keys to protect a device and its data from hacking
    - trusted platform module (TPM) – applied to store encryption keys specific to the host device
  - data in transit encryption:
    - secure sockets layer (SSL) – applied to create an encrypted link between a website and a browser using security keys for businesses to protect the data on their websites
    - transport layer security (TLS) – applied to encrypt end-to-end communication between networks (for example in email, websites and instant messaging)

K1.20 The purpose, criteria and types of back-up involved in risk mitigation:

- purpose:
  - maintaining an up-to-date copy of data to enable future recovery and restoration (full disaster recovery or partial data loss)
- back-up criteria:

Knowledge – What you need to teach

- frequency (for example periodic back-ups)
- source (for example files or data)
- destination (for example internal, external)
- storage (for example linear tape open (LTO), cloud, disk)

- types of back-up:
  - full
  - incremental
  - differential
  - mirror

K1.21 The relationship between organisation policies and procedures and risk mitigation:

- organisational digital use policy:
  - standard operating procedures for:
    - network usage and control (for example monitoring bandwidth, identifying bottlenecks)
    - internet usage (for example restricted access to sites, social media)
    - bring your own device (BYOD)
    - working from home (WFH) (for example DSE assessment)
    - periodic renewal of password
    - software usage (for example updating applications)
- health and safety policy for:
  - standard operating procedures:
    - lone working
    - manual handling/safe lifting (for example moving hardware)
    - working at height
    - fire safety (for example staff training)
    - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013
- change procedure – approval and documentation of all changes
- auditing of policies and standard operating procedures – ensuring all actions are routinely examined (for example to ensure continued compliance)

K1.22 The purpose and application of legislation, industry standards and regulatory compliance, and industry best practice guidelines for the security of information systems in a network cabling context.

Knowledge – What you need to teach

Legislation:

- UK General Data Protection Regulation (UK GDPR):
  - purpose – standardises the way data is used, stored and transferred to protect privacy
  - applications within digital infrastructure:
    - article 1 – subject matter and objectives
    - article 2 – material scope
    - article 3 – territorial scope
    - article 4 – definitions
    - article 5 – principles relating to processing of personal data
    - article 6 – lawfulness of processing
    - article 7–- conditions for consent
- Data Protection Act (DPA) 2018:
  - purpose – implementation of UK GDPR to protect data and privacy
  - applications within digital infrastructure:
    - used fairly, lawfully and transparently
    - used for specified, explicit purposes
    - used in a way that is adequate, relevant and limited to only what is necessary
    - accurate and, where necessary, kept up-to-date
    - kept for no longer than is necessary
    - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- Computer Misuse Act 1990:
  - purpose – protects an individual's computer rights
  - applications within digital infrastructure:
    - unauthorised access to computer materials (point 1 to 3)
    - unauthorised access with intent to commit or facilitate commission of further offences (point 1 to 5)
    - unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (point 1 to 6)

Industry standards and regulatory compliance:

- ISO 27001:

Knowledge – What you need to teach

- purpose – certifiable standard for information security management
- applications within digital infrastructure:
  - UK GDPR/DPA 2018
  - information security
  - information management
  - penetration testing
  - risk assessments

- Payment Card Industry Data Security Standard (PCI DSS):
  - purpose – worldwide standard for protecting business card payments to reduce fraud
  - applications within digital infrastructure:
    - build and maintain a secure network
    - protect cardholder data
    - maintain a vulnerability management program
    - implement strong access control measures
    - regularly monitor and test networks
    - maintain an information security policy

Industry best practice guidelines:

- National Cyber Security Centre (NCSC) '10 Steps to Cyber Security':
  - purpose – inform organisations about key areas of security focus
  - applications within digital infrastructure:
    - user education and awareness
    - home and mobile working
    - secure configuration
    - removable media controls
    - managing user privileges
    - incident management
    - monitoring
    - malware protection
    - network security
    - risk management regime

Knowledge – What you need to teach

- Open Web Application Security Project (OWASP):
  - purpose:
    - implement and review the usage of cyber security tools and resources
    - implement education and training into the general public and for industry experts
    - used as a networking platform
  - applications within digital infrastructure:
    - support users with online security
    - improve security of software solutions

K1.23 Principles of network security and their application to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data:

- the CIA triad – confidentiality, integrity and availability applied to the development of security policies
- identification, authentication, authorisation and accountability (IAAA) – applied to prevent unauthorised access by implementing security policies to secure a network further:
  - applying directory services
  - security authentication process
  - using passwords and security implications
  - identification and protection of data
  - maintaining an up-to-date information asset register

K1.24 Methods of managing and controlling access to digital systems and their application within the design of network security architecture:

- authentication – restricts or allows access based on system verification of user
- firewalls – restricts or allows access to a defined set of services
- intrusion detection system (IDS) – analyses and monitors network traffic for potential threats
- intrusion prevention system (IPS) – prevents access based on identified potential threats
- network access control (NAC) – restricts or allows access based on organisational policy enforcement on devices and users of network
- mandatory access control (MAC) – restricts or allows access based on a hierarchy of security levels
- discretionary access control (DAC) – restricts or allows access based on resource owner preference
- attribute-based access control (ABAC) – restricts or allows access based on attributes or characteristics
- role-based access control (RBAC) – restricts or allows access to resources based on the role of a user

Knowledge – What you need to teach

K1.25 Physical and virtual methods of managing and securing network traffic and their application within the design of network security architecture:

- physical (for example server management, firewalls and cabling):
  - software defined networking (SDN):
    - transport layer security (TLS) (for example used in banking websites)
  - demilitarised zone (DMZ)
  - air gapping
- virtual:
  - virtual LAN (VLAN):
    - VPN (for example intranet, file systems, local network systems)
  - virtual routing and forwarding (VRF)
  - subnets
  - IP security (IPSec)
  - air gapping

K1.26 The principles and applications of cyber security for internet connected devices, systems and networks:

- the confidentiality, integrity and availability (CIA) triad – applied to assess the impact on security of systems (for example data breach)
  - protection and prevention against a cyber attack through secure configuration of a network
  - limiting the network or system exposure to potential cyber attacks
  - detection of cyber attacks and effective logging/auditing to identify impacts
  - appropriate segregation of devices, networks and resources to reduce the impact of a cyber attack

K1.27 Techniques applied to cyber security for internet connected devices, systems and networks:

- wireless security – WPA2 and end-to-end security implemented to monitor access to WiFi systems
- encryption
- virtualisation
- penetration testing
- malware protection
- software updates and patches
- internet gateway security and access control

Knowledge – What you need to teach

- data leakage protection
- multi-factor authentication
- single logout (SLO)

K1.28 The importance of cyber security to organisations and society:

- organisations:
  - protection of:
    - all systems and devices
    - cloud services and their availability
    - personnel data and data subjects (for example employee information, commercially sensitive information)
  - password protection policies for users and systems
  - adherence to cyber security legislation to avoid financial, reputational and legal impacts
  - protection against cybercrime
- society:
  - protection of personal information to:
    - maintain privacy and security
    - protect from prejudices
    - ensure equal opportunities
    - prevent identity theft
  - individuals' rights protected under DPA 2018:
    - be informed about how data is being used
    - access personal data
    - have incorrect data updated
    - have data erased
    - stop or restrict the processing of data
    - data portability (allowing individuals to get and reuse data for different services)
    - object to how data is processed in certain circumstances
  - protection against cybercrime

K1.29 The fundamentals of network topologies and network referencing models and the application of cyber security principles:

- topologies:

Knowledge – What you need to teach

- bus
- star
- ring
- token ring
- mesh
- hybrid
- client-server
- peer-to-peer

- network referencing models:
  - open systems interconnection (OSI) model:
    - application layer
    - presentation layer
    - session layer
    - transport layer
    - network layer
    - data link layer
    - physical layer
  - transmission control protocol/internet protocol (TCP/IP):
    - application layer
    - transport layer
    - network layer
    - network interface layer
- the minimum cyber security standards principles applied to network architecture:
  - identify – management of risks to the security of the network, users and devices:
    - assign cyber security lead
    - risk assessments for systems to identify severity of different possible security risks
    - documentation of configurations and responses to threats and vulnerabilities
  - protect – development and application of appropriate control measures to minimise potential security risks:
    - implementation of anti-virus software and firewall

Knowledge – What you need to teach

- reduce attack surface
- use trusted and supported operating systems and applications
- decommission of vulnerable and legacy systems where applicable
- performance of regular security audits and vulnerability checks
- data encryption at rest and during transmission
- assign minimum access to users
- provide appropriate cyber security training

- detect – implementation of procedures and resources to identify security issues:
  - installation and application of security measures
  - review audit and event logs
  - network activity monitoring
- respond – reaction to security issues:
  - contain and minimise the impacts of a security issue
- recover – restoration of affected systems and resources:
  - back-ups and maintenance plans to recover systems and data
  - continuous improvement review

K1.30 Common vulnerabilities to networks, systems and devices and the application of cyber security controls:

- missing patches, firmware and security updates:
  - application of cyber security controls:
    - patch manager software
    - tracking network traffic
    - test groups/devices to test security
- password vulnerabilities (for example missing, weak or default passwords, no password lockout allowing brute force or dictionary attacks):
  - application of cyber security controls:
    - minimum password requirements in line with up-to-date NCSC guidance (for example length, special character)
    - password reset policy
- insecure basic input-output system (BIOS)/unified extensible firmware interface (UEFI) configuration:
  - application of cyber security controls:

Knowledge – What you need to teach

- review BIOS/UEFI settings
- update BIOS

- misconfiguration of permissions and privileges:
  - application of cyber security controls:
    - testing permissions and access rights to systems
    - scheduled auditing of permissions and privileges (for example remove access of terminated staff)
- unsecure systems due to lack of protection software:
  - application of cyber security controls:
    - protecting against malware (for example virus, worm, trojan, ransomware)
    - update security software
    - monitoring security software
    - buffer overflow
- insecure disposal of data and devices:
  - application of cyber security controls:
    - compliance with Waste Electrical and Electronic Equipment (WEEE) Directive 2013
    - checking and wiping all data devices
- inadequate back-up management:
  - application of cyber security controls:
    - back-up frequency
    - application of appropriate types of back-up
- unprotected physical devices:
  - application of cyber security concepts:
    - install correct software

Skills – What you need to teach

The student must be able to:

S1.1 Apply and maintain procedures and security controls in the installation and maintenance of network cabling to ensure confidentiality, integrity and availability:

Skills – What you need to teach

- implement security controls in a business environment in line with NCSC's 'Cyber Essentials':
  - boundary firewalls
  - secure configuration
  - access control
  - malware protection
  - patch management
- configure and apply appropriate access control methods to physical or virtual networks (for example authentication, MAC, DAC, ABAC, RBAC)
- manage documents and data accurately in accordance with data protection legislation

(GEC5, GDC1, GDC6)

S1.2 Apply and monitor appropriate business control techniques and policies and procedures to ensure personal, physical and environmental security:

- review the identified risk:
  - gather information from system and users
- select, apply and monitor appropriate business control techniques:
  - preventative
  - detective
  - corrective
  - deterrent
  - directive
  - compensating
  - recovery
- comply with relevant regulatory and organisational policies and procedures

(GDC3)

S1.3 Explain the importance of organisational and departmental policies and procedures in respect of adherence to security:

- explain the purpose and application of each policy and procedure, summarising key information and using appropriate technical terms:
  - digital use policy
  - health and safety policy
- explain the potential impact on security if policies and procedures are not adhered to (for example danger to life, privacy)

Skills – What you need to teach

(GEC5, GDC5)

S1.4 Conduct a security risk assessment in line with the risk management process for a system (for example in a local area network cabling):

- assess the system and identify components
- apply the risk management process:
  - identify possible risks within the system
  - calculate the probability and impact of the identified risk
  - analyse and prioritise based on level of risk to system
- record all relevant findings and actions accurately and concisely using appropriate technical terms

(GEC4, GMC5, GDC4)

S1.5 Demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a network cabling context:

- identify, gather and systematically organise information on incidents in preparation for analysis
- process and analyse trends in incident data to identify underlying risks
- identify user profile (for example requirements, ability level)
- identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in networked equipment and devices (for example placement of firewalls)
- monitor and review as part of a continuous improvement process:
  - assign an owner of the risk
  - plan contingencies
- record all relevant findings and actions accurately and concisely using appropriate technical terms

(GEC4, GMC6, GDC4)

Performance outcome 2: Install and test cabling in line with technical and security requirements

Knowledge – What you need to teach

The student must understand:

K2.1 The principles of network cabling:

- representing data electronically:
  - bits
  - bytes
  - packet structures
- data transmission:
  - synchronous transmission
  - asynchronous transmission
  - error detection
  - error correction
  - bandwidth limitation
  - bandwidth noise
  - data compression
  - carrier-sense multiple access with collision detection (CSMA/CD)
  - carrier-sense multiple access with collision avoidance (CSMA/CA)
- network interface cards
- encapsulation:
  - frames
  - packets
  - datagrams
  - addresses
  - sequence numbers
- internet protocol version 4 (IPv4) network and subnets:
  - addressing schemes
  - subnetting
  - subnet masks
- internet protocol version 6 (IPv6):

Knowledge – What you need to teach

- IPv6 address types

K2.2 Tools and equipment used for network cabling:

- network cabling tools:
  - testing tools:
    - multimeter
    - tone generator and probe
    - optical time domain reflectometer (OTDR)
    - light source and power meter
    - spectrum analyser
    - continuity tester
  - terminating tools:
    - crimper
    - copper cable stripper
    - fibre optic stripper
    - cable cutters
    - punch-down tool (for example insulation displacement connector (IDC))
    - screwdrivers
    - fusion splicer
    - fibre cleaning tools (for example alcohol wipes, punching cleaning tools, indirect viewing aids)
    - cleave tool
- physical access equipment:
  - mobile elevating work platforms (MEWPs)
  - low-level access towers
  - step ladders
- fixtures and fittings for telecommunications equipment:
  - cabinets:
    - prebuilt
    - flat pack
  - racks
  - trunking/containment

Knowledge – What you need to teach

K2.3 Networking devices used for network cabling:

- networking devices and components used in installing a network:
  - firewalls
  - routers
  - switches:
    - small form-factor plug (SFP)
  - hubs
  - bridges
  - modems
  - wireless access points (WAPs)
  - media converter
  - wireless range extender
  - voice over IP (VoIP) endpoints
  - CCTV
  - servers
  - network interfaces
  - cabling

K2.4 The factors of structured network cabling design:

- architectural structure of network design:
  - network topology:
    - logical topologies
    - physical topologies
- physical design compliance with standards
- relationship between permanent links and channels
- context of campus distribution
- relationship between passive network design and active network design

K2.5 The purpose and components of a network design specification:

- purpose:
  - to provide the technical overview of the components
- components:

Knowledge – What you need to teach

- customer statement of requirement (SOR)
- bill of materials
- network cabling design documentation:
  - building plans
  - floorplans
  - power and cooling diagram
  - containment layout plans
  - cabling routes plans
- installation administration:
  - labelling
  - documentation
  - certification and warranty
  - declaration of performance of cables
- installation procedures
- contractual penalties
- future proofing/growth strategy

K2.6 The principles of light propagation in fibre cable:

- refraction
- total internal reflection (TIR):
  - transmission of light signal through the core of fibre cable:
    - single mode
    - multi-mode
  - light signal is not absorbed by cladding of fibre cable enabling signal to travel long distances

K2.7 Attenuation within the fibre channel:

- reduction in signal strength when the light signal is transmitted over a distance:
  - measured in decibel (dB)
- considerations:
  - analogue to digital conversion (for example where copper and fibre cable meet)
  - electro-optical conversion
  - synchronous transmission

Knowledge – What you need to teach

- asynchronous transmission
- causes of attenuation:
  - absorption:
    - absorption of light signal by particles in the fibre cable
    - varies by material
    - increases over longer distances
  - scattering:
    - light signal collides with particles inside the fibre cable
    - light signal is absorbed into the cable cladding
  - macrobends – large bends in the fibre cable
  - microbends – small bends in the cable caused by mechanical stress

K2.8 Causes of signal losses as a result of poor handling and installation techniques:

- dirty, faulty or contaminated connectors:
  - unreliable connection
  - no connection
- excessive bending of cabling:
  - under tension
  - not under tension
  - attenuation
- poor quality fibre-optic cables and connectors:
  - interference

K2.9 Principles of Ohm's law and its application to copper network cabling:

- Ohm's law:
  - the relationship between voltage (V), current (I) and resistance (R):
    - V = I x R
    - voltage (V) and current (I) are proportional:
      - as voltage (V) increases, current (I) also increases
    - resistance (R) is the opposing force of current:
      - as resistance (R) increases, current (I) decreases and slows down
- application of Ohm's law to network cabling:

Knowledge – What you need to teach

- Ohm's law describes how a signal is transmitted from point A through a copper cable to point B for it to be received and translated to information
- resistance:
  - varies with length of the cable
  - resistors present within the hardware
  - changes at different frequencies:
    - different size cables for data transmission
    - maximum length cable to ensure efficient signal performance

K2.10 Features of copper and fibre media types and their applications:

- copper cable:
  - features:
    - durable
    - easy to handle
    - cheaper installation
    - high bandwidth
    - can provide power - Power over Ethernet (PoE)
  - applications:
    - telephony distribution
    - maximum limit of 90m (permanent links)
    - short run LAN within 100m total distance (channel links)
  - types:
    - twisted pair (TP):
      - pairs of copper wires twisted together
      - reduces electrical noise (due to twisting of the pairs)
      - used for telephony-based circuits
    - unshielded twisted pair (UTP):
      - no shielding
      - reduces electrical noise (due to twisting of the pairs)
      - reduces electromagnetic interference (EMI)
    - shielded/screened twisted pair (STP):

Knowledge – What you need to teach

- reduces electrical noise (due to twisting of the pairs)
- shielded with insulating coating
- grounds wires
- protects from electromagnetic interference

▪ foil twisted pair (FTP):

- reduces electrical noise (due to twisting of the pairs)
- foil insulation coating

▪ coaxial:

- core copper wire
- plastic insulator around copper wire
- braided sheath to protect from electromagnetic interference
- outer coating to protect inner layers

- fibre cable:
  - features:
    - greater transmission distance
    - higher bandwidth capabilities
    - greater channel carrying capacity
    - lightweight
    - less data degradation
    - materials more expensive but cheaper to maintain long term
    - limited by quality of laser at either end
  - applications:
    - large data transfer rates
    - interconnecting buildings
    - long distance connection points between different sites
  - types:
    - single mode:
      - optical single mode 1 (OS1)
      - optical single mode 2 (OS2)
      - optical fibre core

Knowledge – What you need to teach

- transmit single ray of light
- for use over longer distances

- multi-mode:
  - optical multi-mode 3 (OM3)
  - optical multi-mode 4 (OM4)
  - optical fibre core
  - transmit multiple rays of light
  - for use over shorter distances

K2.11 Advantages of using plenum fire resistant rated cable in network cabling installation over non-fire resistant cable:

- lower toxicity emission
- lower smoke emission
- reduced burning
- reduced material breakdown
- able to withstand higher levels of heat and remain fully operational
- compliant with Construction Products Regulation (CPR)

K2.12 Types and features of connectors that can be applied within network cabling:

- connector types:
  - copper:
    - RJ-45
    - RJ-11
    - Bayonet Neill-Concelman (BNC)
    - DB-9
    - DB-25
    - F-type
  - fibre:
    - local connector (LC)
    - straight tip (ST)
    - standard connector (SC)
    - mechanical transfer registered jack (MT-RJ)

Knowledge – What you need to teach

        - multi-fibre push on (MPO)
    - features of connector types:
        - mating type (male-male, male-female, female-female)
        - locking method/key and ease of connection:
            - latching (for example serial advanced technology attachment (SATA))
            - screw down
            - bayonet (for example BNC)
            - angled physical contact/ultra physical contact (APC/UPC)
        - durability (for example wear and general usage)
        - variation in size
        - insulation between pins (for example strain relief boot)

K2.13 Physical design of transceivers and the criteria for selection:

- physical design of transceivers:
    - small form-factor pluggable (SFP)
    - SFP+
    - gigabit interface converter (GBIC)
    - quad small form-factor pluggable (QSFP)
- criteria for selection of transceivers:
    - simplex/duplex
    - bidirectional
    - bandwidth
    - wave division multiplex
    - dynamic range
    - transfer rate
    - connector type for transceivers
    - housed in standalone unit or hosted in a network switch/router

K2.14 Types of termination points and their applications:

- 66 block:
    - punch-down connection terminal for telephone systems
    - terminate 22 to 26 solid copper wire

Knowledge – What you need to teach

- RJ-21 female connector to receive male-end 25-pair cable
- for Cat3 copper cables
- used to connect cabling in a telephone system

- 110 block:
  - supports higher speed networks than 66 block
  - certified for:
    - Cat5
    - Cat6
    - Cat6a
  - used to terminate on-premises cabling in a structure cabling network
  - supersedes 66 block
- patch panel:
  - contained within a mounted case
  - incoming wires terminate in punch-down blocks
  - patch cable used to interconnect cables by plugging in appropriate jacks
  - handle large volume of copper and fibre cables
  - used as wired network to accommodate ethernet cables

K2.15 Standards for copper and fibre cable, their methods of termination and ethernet deployment standards:

- copper cable standards:

Cable type	Cable rating frequency/MHz	Cable length (max)/m	Ethernet data rate	Ethernet deployment standard
Cat3	16	100	10Mbps	10BASE-T
Cat5	100	100	100Mbps	100BASE-T / 100BASE-TX
Cat5e	100 (up to 350)	100	1Gbps	1000BASE-T
Cat6	250 (up to 550)	100	1Gbps/10Gbps	1000BASE-TX
Cat6a	500 (up to 550)	100	10Gbps	10GBASE-T

Knowledge – What you need to teach

Cat7	600	100	10Gbps	-
RG59	High bandwidth	229	10Mbps	-
RG6	Low bandwidth	305	10Mbps	-

- fibre cable standards:

Ethernet data rate	Wavelength /nm	Cable length (max)/m				
		OS1/OS2	OM1	OM2	OM3	OM4
100Mbps	850	40,000	2,000	2,000	2,000	2,000
1Gbps	850	100,000	275	550	550	1,000
10Gbps	850	40,000	33	82	300	550
40 & 100Gbps	850	40,000	-	-	100	150
1Gbps	1300	-	550	550	550	550
10Gbps	1300	-	300	300	300	300

- termination methods:
  - patching – terminate copper or fibre cable to a patch panel
  - RJ45 – terminate copper cable for ethernet connection
  - splicing – connect fibre cable together:
    - fusion – connection between fibre cables is permanent:
      - used to connect single mode cables
    - mechanical – connection between fibre cables is not permanent:
      - used to connect single mode or multi-mode cables
- termination standards:
  - Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) 568A:
    - American standard
    - pin-out colours adopted by TIA standards
  - TIA/EIA 568B:
    - British and European standard

Knowledge – What you need to teach

- pin-out colours adopted by TIA standards
- crossover:
  - used to connect 2 similar devices together (for example one computer to another)
  - one end of a crossover cable is terminated by TIA/EIA 568B, the other end is terminated by TIA/EIA 568A
  - different colour code pin-out at each end of the cable
- straight-through:
  - used to connect different devices to a network
  - colour codes are the same at both ends of the cable (for example TIA/EIA 568B on both ends)

- ethernet deployment standards:
  - 100BaseT – uses 2 of the 4 pairs
  - 100BaseTX – unidirectional 2 pairs Rx (receive) 2 pairs Tx (transmit)
  - 1000BaseT – bidirectional 4 pair usage
  - 1000BaseT1 – ethernet over single twisted pair (limited length)
  - 1000BaseLX – (LX – long wavelength) single mode and multi-mode
  - 1000BaseSX – (SX – short wavelength) multi-mode only
  - 10GBaseT

K2.16 Maintenance processes of network to ensure efficient running of a network:

- troubleshooting network problems:
  - identify a problem:
    - fault occurs
    - routine monitoring
  - diagnostic:
    - information:
      - investigate user actions
      - network reporting tools
    - analysis of information:
      - compare to previous data
      - compare with similar system/device
    - consider possible causes:

Knowledge – What you need to teach

- eliminate potential causes
- consider remaining possibilities

▪ test remaining possibilities:

- test the shortlist of possible causes
- rule out possible causes that do not work
- identify the correct cause

o resolution:

▪ implement the solution

▪ document the cause and solution on a network plan (for example hardware and software changes)

▪ implement actions to mitigate against cause reoccurring

- hardware and software installation/configuration:
  - o resolution of identified security vulnerabilities:
    - ▪ apply fixes
    - ▪ maintaining compatibility of systems
  - o log all changes to hardware and software:
    - ▪ hardware updates
    - ▪ software updates
  - o inform all necessary stakeholders/users of changes
- monitoring and improving network performance:
  - o network monitoring procedures:
    - ▪ monitor user activity
    - ▪ traffic and load
    - ▪ install network monitoring system (for example packet analysers, firewalls)
    - ▪ track network performance benchmarks
  - o predictive maintenance:
    - ▪ predicting life expectancy of network components and plan to replace
  - o reactive maintenance:
    - ▪ reacting to component failure in a network
  - o run to failure (RTF):

Knowledge – What you need to teach

        - retaining network components until natural failure or upgrade
    - continual service improvements

K2.17 Common types of connectivity and performance failures that can occur in a network:

- network cabling connectivity and performance failures:
    - physical:
        - incorrect cable type (for example unable to transmit signal)
        - incorrect pin-out (for example wire map errors)
        - open/short (for example missing connection or unintended connection)
        - bad port (for example dirty, faulty or contaminated connectors)
        - damaged cables (for example wiring faults, macrobending, microbending)
        - bent pins
        - duplex/speed mismatch (for example incorrect cable)
        - incorrect containment methods (for example reduce signal strength, breach of standards and regulations)
    - technical:
        - attenuation
        - latency
        - jitter
        - cross talk
        - electromagnetic interference (EMI)
        - transceiver mismatch
        - TX/RX reverse (for example polarity mismatch/fibre mismatch)
        - bottlenecks
        - equipment hardware errors
        - light emitting diode (LED) status indicators
- detection of performance failures:
    - cyclical redundancy check
    - encapsulation:
        - frame loss
        - dropped packets

Knowledge – What you need to teach

        - dropped datagrams
        - address conflicts
        - missing sequence numbers
      - analysis of performance benchmark
      - log files

K2.18 Principles of transmission of digital information over copper and fibre cable:

- signal type:
  - electrical-based
  - light-based:
    - laser
    - LED
- security:
  - tampering
  - signal loss
- need for segregation from electrical cables:
  - susceptibility to interference:
    - types of interference (for example electromagnetic impact on signal, static, crosstalk)
    - mitigation techniques (for example shielding, run cables in parallel)
    - adhering to industry standards:
      - BS EN 50174

K2.19 Identification of media supporting other data services and the necessary precautions to prevent interference or damage to systems:

- identifying supporting media:
  - telecommunications
  - security systems (for example CCTV)
  - alarm systems
  - audio visual (AV) systems
  - wireless access points (WAPs)
  - internet of things (IoT) devices
- precautions to mitigate interference or damage to systems:

Knowledge – What you need to teach

- avoid common containment routes
- clearly label service cables
- refer to local authority installation records
- utilise effective change management
- plan and monitor integration of new supporting media:
  - check records
  - IP scanners
  - check cable codes
  - segregate wireless networks

K2.20 Requirements and scope of compliance with legislation, regulations and standards:

- requirement of compliance with legislation, regulations and standards:
  - legal obligations
  - standardisation of work practices and processes (for example production methods, materials used):
    - risk management
  - conforming to industry standards and requirements (for example quality standard)
- scope of related standards:
  - British Standards/European Norm (BS EN):
    - BS EN 50173 (family of standards):
      - standards for generic cabling in different types of premises
    - BS EN 50174 (family of standards):
      - standards for installation specification and quality assurance
      - standards for installation planning and practices inside buildings
      - standards for installation planning and practices outside buildings
    - BS EN 50310:
      - application of equipotential bonding and earthing in buildings with information technology equipment
    - BS EN 60825:
      - standards for safety of optical fibre communication systems (OFCS)
  - British Standards (BS):
    - BS 6701:

Knowledge – What you need to teach

- specification for installation, operation and maintenance
- BS 7671:
- Institute of Electrical and Electronics Engineers (IEEE) Wiring Regulations

- IEEE:
- IEEE 802.16:
- Worldwide Interoperability for Microwave Access (WiMAX)
- IEEE 802.3 series:
- standard specification for ethernet

- International Electrotechnical Commission (IEC):
- IEC60364:
- international standard on electrical installations for buildings

- Telecommunications Industry Association/Electronic Industries Alliance (TIA.EIA):
- TIA/EIA-586-B:
- defines cable categories (Cat3, Cat5, Cat5e, Cat6) and their performance tests and procedures

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC):
- ISO/IEC11801:
- international standard for 'Generic Cabling for Customer Premises', dictates cable class

- European Norm (EN):
- EN50173:
- European standard for generic cabling, consistent with ISO/IEC11801 but includes additional requirements for network cabling

- scope of related legislation and regulations:
- Health and Safety at Work etc Act 1974:
- working with machine tools, working in confined spaces, personal protective equipment (PPE)

- Electricity at Work Regulations 1989:
- working with electricity

- Work at Height Regulations 2005:
- working at height

- Control of Substances Hazardous to Health (COSHH) Regulations 2002:

Knowledge – What you need to teach

- working with hazardous substances
- Confined Spaces Regulation 1997:
  - working in confined spaces
- Personal Protective Equipment Regulation 2018:
  - using appropriate personal protective equipment
- Control of Asbestos Regulations 2012:
  - asbestos-containing materials (ACM)

K2.21 Process and management of the identification of asbestos-containing materials (ACM) are identified during installation work:

- actions required to reduce risk and impact of ACM:
  - application of risk management:
    - identify:
      - stop work immediately
      - informing relevant personnel (for example managers, peers)
      - isolate and restrict access to the area
    - analysis of probability and impact:
      - ensure area is investigated by an asbestos registered professional
    - prioritise and mitigate:
      - outcomes based on investigation data
      - removal or sealant of the material
      - open air checks for contamination and fibres

K2.22 Network cabling inspection parameters and standards:

- network cabling testing standards:
  - TIA/EIA-568-B.2-1:
    - the transmission performance specifications for 4-pair 100Ω Category 6 cabling
  - TIA/EIA-568-B.1-10:
    - the transmission performance specifications for 4-pair 100Ω Augmented Category 6 Cabling Annex I
  - TIA/EIA-TSB-155-A:

Knowledge – What you need to teach

        - guidelines for the assessment and mitigation of installed Category 6 cabling to support 10GBASE-T
    - TIA-1152:
        - requirements for field test instruments and measurements for balanced twisted pair cabling
    - IEC 61935-1:
        - specifies reference measurement procedures for cabling parameters
- network cable certification process:
    - test plan:
        - scope
        - approach
        - resources
        - schedule
    - test equipment:
        - copper test equipment (for example continuity tester, network cabling performance tester, cable certifier)
        - fibre test equipment (for example optical loss test set (OLTS), visible light source, optical time domain reflectometer (OTDR), fibre inspection tool)
    - test types and parameters:
        - copper cable tests (for example wiremap, cable length, near-end crosstalk (NEXT))
        - fibre cable tests (for example tier 1 testing, tier 2 testing, fibre inspection)
    - test results analysis:
- consequences of failing to meet required standards:
    - network:
        - slower network speed
        - increased interference
        - difficult to maintain or upgrade
        - reduced cable lifetime
        - reduced security
    - business:
        - costs of revisit
        - service level agreement penalties

Knowledge – What you need to teach
▪ warranty penalties ▪ reputational damage ▪ delayed payments ▪ failed external audits **K2.23 Impact of poor quality workmanship and non-compliance with network cabling working practices:** • incorrect labelling of circuits, cables and equipment: o increases the difficulty of: ▪ troubleshooting problems ▪ general maintenance ▪ adapting the network for different uses • failure to test all cabling: o damage equipment o premature breakdown o impede services on the network o non-identification of system errors

Skills – What you need to teach

The student must be able to:

S2.1 Design, analyse and interpret a network cabling design specification:

- identify and gather user requirements of the network
- design a network cabling design specification:
  - required components (for example statement of requirements)
- analyse and interpret the network cabling design specification:
  - identify quantity of resources needed (for example people, hardware, software)
  - calculate precise quantities of materials (for example length of cable)
  - assess location of components (for example placement of cables, hardware, network devices)
  - identify potential issues:
    - equipment types
    - quantity of resources and materials
    - location
- the network cabling design specification must:
  - use correct technical language and terms
  - include appropriate plans, diagrams and design documentation to identify installation issues
  - be organised logically and coherently

(GEC1, GEC2, GEC3, GMC1, GMC2, GMC5, GMC7, GDC3)

S2.2 Install and configure network devices on a network:

- interpret a network cabling design specification to identify appropriate location for installation
- checking equipment meets the specification
- confirm physical installation of network devices to a meet specific requirement (for example firewall, router, switch):
  - assess physical space
  - assess access to power
  - assess cooling requirements
- installation of devices into the appropriate cabinets/racks
- test functionality of network devices
- configure network devices to meet specific requirement

(GDC6)

Skills – What you need to teach

S2.3 Apply patching to terminate copper and fibre cables (single and multi-mode) in compliance with industry standards:

- identify type of patching:
  - copper
  - fibre
- connect patch cables to allocated ports on the patch panel
- test patch cables to meet specification using appropriate testing tools
- review termination to ensure it conforms to industry standards:
  - industry standards:
    - TIA/EIA 568A
    - TIA/EIA 568B
    - BS EN 61300

S2.4 Demonstrate effective application of networking tools for a specific purpose in a network cabling context:

- assess the parameters of the work being carried out
- select appropriate tool to meet parameters:
  - testing tools (for example multimeter, tone generator and probe)
  - terminating tools (for example crimper, copper cable stripper, fibre optic stripper)
- demonstrate safe application in compliance with manufacturers' guidelines of use

(GDC6)

S2.5 Prepare, construct, arrange and install fixtures and fittings accurately to meet a specific network cabling requirement:

- interpret a network cabling design specification for the installation of fixtures and fittings for telecommunications equipment
- compare the physical location against the specification:
  - assess physical space
  - assess access to power
  - assess cooling requirements
- construct and install appropriate cabinets/racks in compliance with manufacturers' guidelines and instructions:
  - prebuilt or flat pack
- install additional fixtures and fittings (for example trucking and containment)

Skills – What you need to teach

- test all fixtures and fittings to ensure compliance with legislation, installation and safety requirements
- arrange the equipment to meet the specification within the racks

(GMC7)

S2.6 Carry out cable testing, applying appropriate testing tools, in accordance with equipment manufacturers' procedures and in compliance with TIA/EIA standards:

- identify the physical characteristics to be tested:
  - copper
  - fibre
- identify the appropriate cable specification
- apply appropriate testing methods to identified cable:
  - copper cabling testing and parameters (for example wiremap, cable length):
    - identify the appropriate testing tools
    - apply copper test equipment in compliance with manufacturers' guidelines and industry standards (for example continuity tester, network cabling performance tester, cable certifier)
  - fibre optic cabling testing:
    - applying an optical loss test set (tier 1) in compliance with manufacturers' guidelines and industry standards
    - applying an optical time domain reflectometer (OTDR) (tier 2) in compliance with manufacturers' guidelines and industry standards
    - applying a fibre inspection tool in compliance with manufacturers' guidelines and industry standards
- systematically record and organise test results

(GEC3, GMC4, GMC5)

S2.7 Analyse and interpret copper and fibre test results:

- gather required data for analysis
- use appropriate software to process test results
- compare results against manufacturers' guidelines to ensure they are within accepted specification ranges
- analyse and interpret test results
- record and summarise reasoned conclusions based on the interpretation of data to meet intended purpose and user requirements

(GEC1, GEC3, GEC4, GEC5, GMC1, GMC6, GMC8, GDC4)

Skills – What you need to teach

S2.8 Apply the risk management process to work safely at height using equipment to facilitate installation of network cabling:

- undertake the risk management process to identify risk and record all outcomes:
  - identification
  - probability
  - impact
  - prioritisation
  - mitigation
- demonstrate working at height in a safe manner using mobile elevating work platforms (MEWPs) in compliance with Health and Safety at Work etc Act 1974 regulations
- assemble prefabricated low level access towers in compliance with manufacturers' guidelines
- inspect prefabricated low level access towers in compliance with manufacturers' guidelines
- operate prefabricated low level access towers in compliance with manufacturers' guidelines
- dismantle prefabricated low level access towers in compliance with manufacturers' guidelines

(GMC6)

S2.9 Apply the risk management process to ensure safe practices and procedures for working in confined spaces, in compliance with relevant health and safety legislation and regulations (for example Health and Safety at Work etc Act 1974, Confined Spaces Regulations 1997):

- undertake the risk management process to identify risk and record all outcomes:
  - identification
  - probability
  - impact
  - prioritisation
  - mitigation
- identify and apply appropriate PPE in compliance with legislation (for example Health and Safety at Work etc Act 1974):
  - maintaining PPE in compliance with manufacturers' guidelines
- record and logically organise all relevant findings and actions accurately and concisely using appropriate technical terms to inform future policies and procedures
  - summarise key information

(GEC1, GEC3, GEC4, GMC10)

Skills – What you need to teach

S2.10 Explain the risk management process that must be applied if asbestos-containing materials (ACM) are identified whilst installation work is being carried out:
• undertake the risk management process to identify risk and record all outcomes:
  o identification – request access to onsite register
  o analysis of probability and impact
  o prioritisation and mitigation
• record and logically organise all relevant findings and actions accurately and concisely using appropriate technical terms to inform future policies and procedures
  o summarise key information
(GEC1, GEC3, GEC4, GMC10)

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach

The student must understand:

K3.1 Types of sources of knowledge that can be applied within network cabling:

- academic publications (for example textbooks, research journals and periodicals)
- supplier literature (for example handbooks or online articles for specific devices, computers or laptops)
- search engines (for example Google, Bing)
- websites (for example wikis, forums, Stack Overflow, manufacturers' websites)
- social media (for example company profiles for Twitter, Facebook and LinkedIn)
- blogs (for example reviews of new technologies, opinions on topical issues in the digital sector)
- vlogs (for example demonstrations, tutorials on digital technologies)
- professional networks (for example digital transformation networking events/conferences)
- e-learning (for example massive open online courses (MOOCs), recognised vendor qualifications, Cisco)
- peers (for example colleagues, network contacts, other industry professionals)

K3.2 The factors of reliability and validity to be applied to legitimise the use of sources of knowledge:

- industry-certified accreditation (for example Cisco certified network associate (CCNA1), Microsoft technology associate (MTA), network fundamentals)
- appropriateness
- evidence-based:
  - citations
- relevant context
- credibility of author:
  - affiliated to specific bodies (for example government, industry regulators)
  - reputation
  - experience (for example relevant qualification in subject)
- target audience – produced with specific audience requirements taken into consideration (for example use of technical/non-technical terminology)
- publication:
  - version (for example use of the current version)

Knowledge – What you need to teach

- date of publication (for example if the content is outdated)

K3.3 The factors of bias:

- types of conscious and unconscious bias:
  - author/propriety bias – unweighted opinions of the author or owner
  - confirmation bias – sources support a predetermined assumption
  - selection bias – selection of sources that meets specific criteria
  - cultural bias – implicit assumptions based on societal norms
- indicators of bias within sources:
  - partiality
  - prejudice
  - omission
- bias reduction:
  - based on fact/evidence
  - inclusive approach:
    - full representation of demographics
  - objectivity

K3.4 Process of critical thinking and the application of evaluation techniques and tools:

- process of critical thinking:
  - identification of relevant information:
    - different arguments, views and opinions
  - analysis of identified information:
    - identify types of bias and objectivity
    - understand links between information and data
  - selection of relevant evaluation techniques and tools
  - evaluation of findings and drawing of conclusions
  - recording of conclusions
- evaluation techniques:
  - formative evaluation
  - summative evaluation
  - qualitative (for example interviews, observations, workshops)

Knowledge – What you need to teach

- quantitative (for example experiments, surveys, statistical analysis)
- benchmarking
- corroboration:
  - cross-referencing
- triangulation

- evaluation tools:
  - gap analysis
  - KPI analysis
  - score cards
  - observation reports
  - user diaries
  - scenario mapping
  - self-assessment frameworks
  - maturity assessments

K3.5 Methods of communication and sharing knowledge and their application within a network cabling context:

- integrated and standalone IT service management tools:
  - incident and problem management systems
  - change management systems
- knowledge bases and knowledge management systems
- wikis and shared documents
- shared digital workspaces
- telephone
- instant messaging
- email
- video conferencing
- digital signage
- social media:
  - organisational
  - public

Knowledge – What you need to teach

- personal
- blogs
- community forums
- project management tools (for example issue logs, Gantt charts, Kanban boards, burndown charts):
  - policy, process and procedure documents

Skills – What you need to teach

The student must be able to:

S3.1 Identify sources of knowledge and apply factors that legitimise their use to meet requirements in a network cabling context:

- identify and clarify the parameters of the requirements
- identify appropriate sources of knowledge (up to 3) (for example search engines, blogs)
- apply the factors of reliability and validity to identified sources (for example authority, date of publication)
- assess and review potential bias of sources
- assess and review the identified sources' appropriateness to meet the requirements

(GEC4, GDC1)

S3.2 Search for information to support a topic or scenarios within network cabling and corroborate information across multiple sources:

- identify and clarify the parameters of the search (for example explore the future of the digital economy, identify trends in big data)
- identify the sources of data that contain the required information
- safely and securely search sources for the information required
- corroborate sources by applying cross-referencing across multiple sources
- apply reliability and validity factors
- assess and review potential bias of sources

(GEC4, GDC5)

S3.3 Select and apply techniques and tools to support evaluation in a network cabling context:

- identify and clarify the parameters of the evaluation
- select appropriate techniques and tools to support the evaluation

Skills – What you need to teach

- apply the selected techniques and use the appropriate tools to support the evaluation
- record the findings of the evaluation for the requirement

(GEC4, GDC2)

S3.4 Compare options of sources and rationalise the actions taken to ensure the reliability and validity of sources:

- identify the sources for comparison
- apply the relevant reliability and validity factors to the sources
- compare the outcomes of the validity and reliability actions
- explain and recommend the choice of action to ensure the sources are reliable and valid, using appropriate technical terms

(GEC1, GEC3, GEC5, GMC5, GDC3)

S3.5 Identify and understand bias when using sources of knowledge in a specific network cabling context:

- identify the types of bias (for example confirmation, unconscious)
- identify the indicators of bias within the source
- explain clearly and concisely how bias has been created within the source
- explain clearly and concisely how bias can be avoided within sources

(GEC1, GEC3, GEC5, GMC6, GDC3)

S3.6 Demonstrate critical thinking within a network cabling context:

- apply the process of critical thinking to meet requirements:
  - identify relevant information
  - analyse the information
  - select and apply appropriate evaluation techniques and tools
  - evaluate findings
  - logically organise and record conclusions

(GEC1, GEC3, GMC5, GMC6, GMC8, GDC3, GDC4)

Occupational specialism: Digital Support

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The ‘K’ and ‘S’ indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Install, configure and support software applications and operating systems
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data

Knowledge – What you need to teach

The student must understand:

K1.1 The types of preventative business control techniques in protecting the digital security of an organisation:

- preventative control techniques:
  - physical:
    - specialist locks (anti-picking)
    - barriers (for example fencing, bollards)
    - gates
    - cages
    - flood defence systems
    - temperature control (for example air conditioning)
  - combined – managed access:
    - card readers
    - biometric
    - video
    - pin/passcodes
  - administrative, policies and procedures:
    - separation of duties and relevance of role-based access
  - technical – domains and security policies:
    - whitelisting

Knowledge – What you need to teach

- blacklisting
- access control lists
- sandboxing
- device hardening
- certificate authority

K1.2 The types of detective business control techniques in protecting the digital security of an organisation:

- detective control techniques:
  - physical:
    - CCTV
    - motion sensors
  - administrative, policies and procedures:
    - logs (for example logs of temperature in server room, error logs)
    - review/audit (for example people entering and leaving the facilities)

K1.3 The types of corrective business control techniques in protecting the digital security of an organisation:

- corrective control techniques:
  - physical:
    - fire suppression (for example sprinklers, extinguishers)
    - gas suppression (for example inert and chemical gas systems)
  - administrative, policies and procedures:
    - standard operating procedure (for example actions taken when a fire is identified)

K1.4 The types of deterrent business control techniques in protecting the digital security of an organisation:

- deterrent control techniques:
  - physical:
    - security guards
    - alarm systems
    - visible surveillance systems
  - administrative, policies and procedures:
    - standard operating procedure (for example setting alarm system, fire drill)

Knowledge – What you need to teach

- employment contracts stipulating codes of conduct
- acceptable usage policies

K1.5 The types of directive business control techniques in protecting the digital security of an organisation:

- directive control techniques:
  - physical:
    - signage
    - mandatory ID badge display (employees and visitors)
  - administrative, policies and procedures:
    - agreement types
    - general security policies and procedures
    - regular and compulsory staff training (for example human firewall training)

K1.6 The types of compensating business control techniques in protecting the digital security of an organisation:

- compensating control techniques:
  - physical:
    - temperature controls (for example air conditioning)
  - administrative, policies and procedures:
    - role-based awareness training
    - standard operating procedures (for example environmental control monitoring)

K1.7 Components of a disaster recovery plan in protecting the digital security of an organisation:

- disaster recovery plan (DRP) components:
  - physical:
    - back-ups
    - off-site alternative storage of servers
  - administrative, policies and procedures of a DRP supported by an organisational business continuity plan (BCP):
    - ensuring all systems maintain functionality (for example arranging hardware)
    - ensuring users can access systems away from the main building site
    - deploying back-ups to maintain data integrity
    - ensuring digital changes continue to meet business needs

Knowledge – What you need to teach

- managing assets across the network and logging changes (for example tagging and logging laptops)
- reporting infrastructure changes to management

K1.8 The types of impacts that can occur within an organisation as a result of threats and vulnerabilities:

- danger to life – breaches in health and safety policies (for example injury and death)
- privacy – breaches of data (for example compromised confidential business data, identity theft)
- property and resources – damage to property and systems
- economic – financial loss or impairment
- reputation – damage to brand and business value
- legal – fines, prosecution

K1.9 The potential vulnerabilities in critical systems:

- unauthorised physical access to network ports
- user account control
- single point of failure
- open port access:
  - universal serial bus (USB)
  - optical media:
    - compact disc (CD)
    - digital versatile disc (DVD)
  - network ports
- wireless networks

K1.10 The impact of measures and procedures that are put in place to mitigate threats and vulnerabilities:

- measures:
  - recovery time objective (RTO)
  - recovery point objective (RPO)
  - mean time between failure (MTBF)
  - mean time to repair (MTTR)
- procedures:
  - standard operating procedure (SOP):

Knowledge – What you need to teach

- installation procedure
- back-up procedure
- set-up procedure

- service level agreement (SLA):
  - system availability and uptime
  - response time and resolution timescales

K1.11 The process of risk management:

- process:
  - identification – identifying potential risk or threats and vulnerabilities
  - probability – likelihood of occurrence (for example high, medium, low)
  - impact – assess damage that can occur (for example asset value)
  - prioritisation – rank risks based on the analysis of probability and impact, ownership of risk
  - mitigation – reducing probability or impact of risk

K1.12 Approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – non-numeric:
    - determine severity using RAG rating:
      - red – high risk requiring immediate action
      - amber – moderate risk that needs to be observed closely
      - green – low risk with no immediate action required
  - quantitative – numeric:
    - analyse effects of risk (for example cost overrun, resource consumption)
- tools:
  - fault tree analysis
  - impact analysis
  - failure mode effect critical analysis
  - annualised loss expectancy (ALE)
  - Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)
  - strength, weakness, opportunity, threat (SWOT) analysis

Knowledge – What you need to teach

- risk register – risk is identified and recorded using a RAG rating
- risk matrix – used to calculate the RAG rating for a risk

K1.13 Factors involved in threat assessment for the mitigation of threats and vulnerabilities:

- environmental:
  - extreme weather
  - natural disaster
  - animals (for example rodent in server room)
  - humidity
  - air quality
- manmade:
  - internal:
    - malicious or inadvertent activity from employees and contractors
  - external:
    - malware
    - hacking
    - social engineering
    - third-party organisations
    - terrorism
- technological:
  - technology failures and faults:
    - misconfigured devices
    - WiFi dropouts
    - inaccessible systems
    - VPN not connecting
    - expired passwords
  - device failure and faults (for example laptops, tablets, telephones):
    - hard disk failure
    - RAM failure
    - damaged peripherals
  - system failures and faults:

Knowledge – What you need to teach

        - software breakages/corruption
        - inaccessible websites
    - impact of technical change:
        - potential downtime
        - system/software upgrades
        - misconfigured systems
- political:
    - changes/amendments in legislation

K1.14 The purpose of risk assessment in a digital support context:

- purpose:
    - to identify and reduce risk by:
        - implementing Health and Safety Executive (HSE) guidelines to projects (for example supporting users with safe ergonomic equipment usage and accessibility)
        - investigating risks within the project environment (for example undertaking a PESTLE analysis)
        - internal and external risk identification (for example system access for employees and contractors)
        - quantification of impact on asset value (for example financial loss as a result of downtime)

K1.15 Types of risk response within a digital support context:

- types of response:
    - accept – the impact of the risk is deemed acceptable
    - avoid – change scope to avoid identified risk
    - mitigate – reduce the impact or probability of the identified risk
    - transfer – contractually outsource the risk to another party

K1.16 The process of penetration testing within digital support:

- penetration testing (for example wireless network tests):
    - customer engagement
    - information gathering
    - discovery and scanning
    - vulnerability testing
    - exploitation

Knowledge – What you need to teach

- final analysis and review
- utilise the test results

K1.17 The considerations in the design of a risk mitigation strategy:

- risk response (for example accept, avoid, mitigate or transfer the risk)
- user profile (for example requirements, ability level)
- cost and benefit
- assign an owner of the risk
- escalation to appropriate authority within organisation
- planning contingencies
- monitoring and reviewing process

K1.18 The purpose of technical security controls as risk mitigation techniques and their applications to business risks within a digital support context:

- purpose – to improve network security for users and systems
- technical security controls and their applications:
  - 5 cyber essentials controls:
    - access control – restricting access to a minimum based on user attributes (for example principle of least privilege, username and password management)
    - patch management – maintaining system and software updates to current levels
    - malware protection – maintaining up-to-date anti-malware/anti-virus software and regular scanning
    - boundary firewalls and internet gateways – restricting the flow of traffic in systems
    - secure configuration – ensuring user only has required functionality (for example removing unnecessary software, configuration to limit web access)
  - device hardening – removing unneeded programs, accounts functions, applications, ports, permissions and access
  - remote monitoring and management (RMM) (for example end user devices)
  - vulnerability scanning (for example port scanning, device scanning)

K1.19 The purpose and types of encryption as a risk mitigation technique and their applications:

- purpose – to store and transfer data securely using cryptography
- types of encryption and their applications:
  - asymmetric encryption – applied to send private data from one user to another (for example encrypted email systems)

Knowledge – What you need to teach

- symmetric encryption – applied to encrypt and decrypt a message using the same key (for example card payment systems)
- data at rest encryption:
  - full disk encryption – applied to encrypt the contents of an entire hard drive using industry standard tool (for example Windows, macOS)
  - HSM – safeguards digital keys to protect a device and its data from hacking
  - TPM – applied to store encryption keys specific to the host device
- data in transit encryption:
  - SSL – applied to create an encrypted link between a website and a browser using security keys for businesses to protect the data on their websites
  - TLS – applied to encrypt end-to-end communication between networks (for example in email, websites and instant messaging)

K1.20 The purpose, criteria and types of back-up involved in risk mitigation:

- purpose:
  - maintaining an up-to-date copy of data to enable future recovery and restoration (for example full disaster recovery or partial data loss)
- back-up criteria:
  - frequency (for example periodic back-ups)
  - source (for example files or data)
  - destination (for example internal, external)
  - storage (for example linear tape open (LTO), cloud, disk)
- types of back-up:
  - full
  - incremental
  - differential
  - mirror

K1.21 The relationship between organisational policies and procedures and risk mitigation:

- organisational digital use policy:
  - standard operating procedures for:
    - network usage and control (for example monitoring bandwidth, identifying bottlenecks)
    - internet usage (for example restricted access to sites, social media)
    - bring your own device (BYOD)

Knowledge – What you need to teach

- working from home (WFH) (for example DSE assessment)
- periodic renewal of password
- software usage (for example updating applications)

- health and safety policy for:
  - standard operating procedures:
    - lone working
    - manual handling/safe lifting (for example moving hardware)
    - working at height
    - fire safety (for example staff training)
    - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013
- change procedure – approval and documentation of all changes
- auditing of policies and standard operating procedures – ensuring all actions are routinely examined (for example to ensure continued compliance)

K1.22 The purpose and application of legislation, industry standards and regulatory compliance, and industry best practice guidelines for the security of information systems in the context of digital support.

Legislation:

- UK General Data Protection Regulation (UK GDPR):
  - purpose – standardises the way data is used, stored and transferred to protect privacy
  - applications within digital support:
    - article 1 – subject matter and objectives
    - article 2 – material scope
    - article 3 – territorial scope
    - article 4 – definitions
    - article 5 – principles relating to processing of personal data
    - article 6 – lawfulness of processing
    - article 7 – conditions for consent
- Data Protection Act (DPA) 2018:
  - purpose – implementation of UK GDPR to protect data and privacy
  - applications within digital support:
    - used fairly, lawfully and transparently

Knowledge – What you need to teach

- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up-to-date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

- Computer Misuse Act 1990:
  - purpose – protects an individual's computer rights
  - applications within digital support:
    - unauthorised access to computer materials (point 1 to 3)
    - unauthorised access with intent to commit or facilitate commission of further offences (point 1 to 5)
    - unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (point 1 to 6)

Industry standards and regulatory compliance:

- ISO 27001:
  - purpose – certifiable standard for information security management
  - applications within digital support:
    - UK GDPR/DPA 2018
    - information security
    - information management
    - penetration testing
    - risk assessments
- Payment Card Industry Data Security Standard (PCI DSS):
  - purpose – worldwide standard for protecting business card payments to reduce fraud
  - applications within digital support:
    - build and maintain a secure network
    - protect cardholder data
    - maintain a vulnerability management program
    - implement strong access control measures
    - regularly monitor and test networks

Knowledge – What you need to teach

- maintain an information security policy

Industry best practice guidelines:

- National Cyber Security Centre (NCSC) '10 Steps to Cyber Security':
  - purpose – inform organisations about key areas of security focus
  - applications within digital support:
    - user education and awareness
    - home and mobile working
    - secure configuration
    - removable media controls
    - managing user privileges
    - incident management
    - monitoring
    - malware protection
    - network security
    - risk management regime
- Open Web Application Security Project (OWASP):
  - purpose:
    - implements and reviews the usage of cyber security tools and resources
    - implements education and training into the general public and for industry experts
    - used as a networking platform
  - applications within digital support:
    - support users with online security
    - improve security of software solutions

K1.23 Principles of network security and their application to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data:

- the CIA triad – confidentiality, integrity and availability applied to the development of security policies
- IAAA (identification, authentication, authorisation and accountability) – applied to prevent unauthorised access by implementing security policies to secure a network further:
  - applying directory services
  - security authentication process
  - using passwords and security implications

Knowledge – What you need to teach

- identification and protection of data
- maintaining an up-to-date information asset register

K1.24 Methods of managing and controlling access to digital systems and their application within the design of network security architecture:

- authentication – restricts or allows access based on system verification of user
- firewalls – restricts or allows access to a defined set of services
- intrusion detection system (IDS) – analyses and monitors network traffic for potential threats
- intrusion prevention system (IPS) – prevents access based on identified potential threats
- network access control (NAC) – restricts or allows access based on organisational policy enforcement on devices and users of network
- mandatory access control (MAC) – restricts or allows access based on a hierarchy of security levels
- discretionary access control (DAC) – restricts or allows access based on resource owner preference
- attribute-based access control (ABAC) – restricts or allows access based on attributes or characteristics
- role-based access control (RBAC) – restricts or allows access to resources based on the role of a user

K1.25 Physical and virtual methods of managing and securing network traffic and their application within the design of network security architecture:

- physical (for example businesses utilising servers, firewalls and cabling):
  - software defined networking (SDN):
    - transport layer security (TLS) (for example used for banking websites)
  - demilitarised zone (DMZ)
  - air gapping
- virtual:
  - virtual LAN (VLAN):
    - virtual private network (VPN) (for example intranet, file systems, local network systems)
  - virtual routing and forwarding (VRF)
  - subnets
  - IP security (IPSec)
  - air gapping

Knowledge – What you need to teach

K1.26 The principles and applications of cyber security for internet connected devices, systems and networks:

- the confidentiality, integrity and availability (CIA) triad – applied to assess the impact on security of systems (for example data breach)
    - protection and prevention against a cyber attack through secure configuration of a network
    - limiting the network or system exposure to potential cyber attacks
    - detection of cyber attacks and effective logging/auditing to identify impacts
    - appropriate segregation of devices, networks and resources to reduce the impact of a cyber attack

K1.27 Techniques applied to cyber security for internet connected devices, systems and networks:

- wireless security – WPA2 and use of end-to-end security implemented to monitor access to WiFi systems
- device security – password/authentication implemented to improve device security
- encryption
- virtualisation
- penetration testing
- malware protection
- anti-virus protection
- software updates and patches
- multi-factor authentication
- single logout (SLO)

K1.28 The importance of cyber security to organisations and society:

- organisations:
    - protection of:
        - all systems and devices
        - cloud services and their availability
        - personnel data and data subjects (for example employee information, commercially sensitive information)
    - password protection policies for users and systems
    - adherence to cyber security legislation to avoid financial, reputational and legal impacts
    - protection against cybercrime
- society:

Knowledge – What you need to teach
○ protection of personal information to: ▪ maintain privacy and security ▪ protect from prejudices ▪ ensure equal opportunities ▪ prevent identity theft ○ individuals' rights protected under DPA 2018: ▪ be informed about how data is being used ▪ access personal data ▪ have incorrect data updated ▪ have data erased ▪ stop or restrict the processing of data ▪ data portability (allowing individuals to get and reuse data for different services) ▪ object to how data is processed in certain circumstances ○ protection against cybercrime **K1.29 The fundamentals of network topologies and network referencing models and the application of cyber security principles:** • topologies: ○ bus ○ star ○ ring ○ token ring ○ mesh ○ hybrid ○ client-server ○ peer-to-peer • network referencing models: ○ open systems interconnection (OSI) model: ▪ application layer ▪ presentation layer ▪ session layer

Knowledge – What you need to teach

        - transport layer
        - network layer
        - data link layer
        - physical layer
    - transmission control protocol/internet protocol (TCP/IP):
        - application layer
        - transport layer
        - network layer
        - network interface layer
- the minimum cyber security standards principles applied to network architecture:
    - identify – management of risks to the security of the network, users and devices:
        - assign cyber security lead
        - risk assessments for systems to identify severity of different possible security risks
        - documentation of configurations and responses to threats and vulnerabilities
    - protect – development and application of appropriate control measures to minimise potential security risks:
        - implementation of anti-virus software and firewall
        - reduce attack surface
        - use trusted and supported operating systems and applications
        - decommission of vulnerable and legacy systems where applicable
        - performance of regular security audits and vulnerability checks
        - data encryption at rest and during transmission
        - assign minimum access to users
        - provide appropriate cyber security training
    - detect – implementation of procedures and resources to identify security issues:
        - installation and application of security measures
        - review audit and event logs
        - network activity monitoring
    - respond – reaction to security issues:
        - contain and minimise the impacts of a security issue

Knowledge – What you need to teach

- recover – restoration of affected systems and resources:
  - back-ups and maintenance plans to recover systems and data
  - continuous improvement review

K1.30 Common vulnerabilities to networks, systems and devices and the application of cyber security controls:

- missing patches, firmware and security updates:
  - application of cyber security controls:
    - patch manager software
    - tracking network traffic
    - test groups/devices to test security
- password vulnerabilities (for example missing, weak or default passwords, no password lockout allowing brute force or dictionary attacks):
  - application of cyber security controls:
    - minimum password requirements in line with up-to-date NCSC guidance (for example length, special character)
    - password reset policy
- insecure basic input-output system (BIOS)/unified extensible firmware interface (UEFI) configuration:
  - application of cyber security controls:
    - review BIOS/UEFI settings
    - update BIOS
- misconfiguration of permissions and privileges:
  - application of cyber security controls:
    - testing permissions and access rights to systems
    - scheduled auditing of permissions and privileges (for example remove access of terminated staff)
- unsecure systems due to lack of protection software:
  - application of cyber security controls:
    - protecting against malware (for example virus, worm, trojan, ransomware)
    - update security software
    - monitoring security software
    - buffer overflow

Knowledge – What you need to teach

- insecure disposal of data and devices:
  - application of cyber security controls:
    - compliance with Waste Electrical and Electronic Equipment (WEEE) Directive 2013
    - checking and wiping all data devices
- inadequate back-up management:
  - application of cyber security controls:
    - back-up frequency
    - application of appropriate types of back-up
- unprotected physical devices:
  - application of cyber security controls:
    - install correct software

Skills – What you need to teach

The student must be able to:

S1.1 Apply and maintain procedures and security controls in the installation, configuration and support of end user services to ensure confidentiality, integrity and availability:

- set up a domain services environment with security controls (for example group-based security and permissions, password complexity)
- set up and deploy a certificate authority (for example directory certificate services – install onto PC)
- implement security controls in a business environment in line with NCSC cyber essentials:
  - boundary firewalls
  - secure configuration (for example enabling multi-factor authentication (MFA))
  - access control
  - malware protection
  - patch management
- configure and apply appropriate access control methods to end user devices (for example authentication, MAC, DAC, ABAC, RBAC)
- manage documents and data accurately in accordance with data protection legislation

(GEC5, GDC1, GDC5, GDC6)

Skills – What you need to teach

S1.2 Apply and monitor appropriate business control techniques and policies and procedures to ensure personal, physical and environmental security:

- review the identified risk:
  - gather information from system and users
- select, apply and monitor appropriate business control techniques:
  - preventative
  - detective
  - corrective
  - deterrent
  - directive
  - compensating
  - recovery
- comply with relevant regulatory and organisational policies and procedures

(GDC3)

S1.3 Explain the importance of organisational and departmental policies and procedures in respect of adherence to security:

- explain the purpose and application of each policy and procedure, summarising key information and using appropriate technical terms:
  - digital use policy
  - health and safety policy
- explain the potential impact on security if policies and procedures are not adhered to (for example danger to life, privacy)

(GEC5, GDC5)

S1.4 Install and configure software end user devices (for example servers, desktop computers) to identify and mitigate vulnerabilities:

- install and configure software on end user devices:
  - vulnerability scanning software (for example port scanning software, device scanning software)
  - anti-malware software
  - firewall software
- apply device hardening to remove unnecessary software
- check installation and configuration on end user devices

(GEC4, GDC1, GDC6)

Skills – What you need to teach

S1.5 Conduct a security risk assessment in line with the risk management process for a system (for example BYOD):

- assess the system and identify components
- apply the risk management process:
  - identify possible risks within the system
  - calculate the probability and impact of the identified risk
  - analyse and prioritise based on level of risk to system
  - record all relevant findings and actions accurately and concisely using appropriate technical terms

(GEC4, GMC6, GDC4)

S1.6 Demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a digital support context:

- identify, gather and systematically organise information on incidents in preparation for analysis
- process and analyse trends in incident data to identify underlying risks
- identify user profile (for example requirements, ability level)
- identify and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices (for example installing RMM software, device hardening)
- monitor and review as part of a continuous improvement process:
  - assign an owner of the risk
  - plan contingencies
  - update devices with current security software
  - interpret the outputs of penetration testing
  - record all relevant findings and actions accurately and concisely using appropriate technical terms

(GEC4, GMC5, GDC4)

S1.7 Demonstrate operating data systems effectively to meet the requirements of business within a digital support context:

- identify and clarify the parameter of requirements
- identify data systems relevant to requirements
- apply appropriate security controls and procedures when operating data systems
- comply with all organisational policies and procedures when operating data systems

(GEC4, GMC10, GDC1, GDC5, GDC6)

Performance outcome 2: Install, configure and support software applications and operating systems

Knowledge – What you need to teach

The student must understand:

K2.1 The values of agile methodologies and work practices:

- individuals and interactions over processes and tools
- working software over comprehensive documentation
- customer collaboration over contract negotiation
- responding to change over following a plan

K2.2 The applications of agile methodologies and work practices in support of continuous innovation and development in a digital environment:

- Scrum:
  - defined roles, events, artefacts and rules
  - applies daily scrums
  - workloads are broken down into sprints
- Kanban:
  - manages workloads by balancing demands with available capacity
  - identifies bottlenecks in workload
  - manages work using a Kanban board
  - uses work in progress (WIP) limits to prevent over-commitment
- dynamic systems development method (DSDM):
  - fixed cost, quality and time
  - uses MoSCoW in the prioritisation of scope
- feature-driven development:
  - breaks down development into smaller features
  - plans, designs and builds by feature
- Crystal:
  - focuses on communications and interactions between people over processes and tools
- Lean (7 principles):
  - eliminate waste
  - build in quality

Knowledge – What you need to teach

- create knowledge
- defer commitment
- deliver fast
- respect people
- optimise the whole

- extreme programming (XP):
  - advocates frequent releases in short development cycles
  - introduces check points when new customer requirements can be adopted
  - uses planning and feedback loops

K2.3 The incorporation of digital technologies by organisations into key areas of business operations and the implications for digital support roles:

- key areas:
  - finance:
    - budget/finance dashboards
    - invoicing processes
    - online expense tracking
  - sales and marketing:
    - customer relationship management (CRM) systems
    - social media management and tools
  - operations:
    - performance dashboards
    - online ticket systems
  - human resources:
    - personnel management systems
    - digital training
  - communications:
    - video conferencing
    - email
    - collaborative platforms
  - research and development:

Knowledge – What you need to teach

- access to information
- development environments (for example computer-aided design (CAD), integrated development environment (IDE)

- implications for digital support roles:
  - increased demand for support due to organisational system's reliance on digital systems
  - increased training needs of workforce due to reliance on digital competencies and digital skills
  - increased requirement for CPD to support changing systems and technologies
  - requirement to operate and maintain changing digital information systems to support the organisation to collect, store, maintain and distribute information

K2.4 The application of service functions in creating a domain within a networked environment:

- active directory domain services (AD DS):
  - active directory – provides functionality to centrally manage and organise user and device accounts, security groups and distribution lists, contained in organisational units (OUs)
  - group policy – provides functionality to create group policy objects (GPOs) which can be applied to OUs. GPOs can be applied to deploy settings and files to users' profiles and devices, based on their OU
- dynamic host configuration protocol (DHCP) – a network management protocol to assign IP addresses and network configuration to a network client device
- domain name system (DNS) – for the translation of hostnames to IP addresses
- file server and distributed file system (DFS) – to provide shared disk access and manage permissions
- print server – to provide shared printer access
- mail servers – manage emails to/from client mailboxes
- certificate authorities – application of digital certificates to certify the ownership of a public key for use in encryption

K2.5 The applications and processes of content management system (CMS) and the methods used to identify and resolve user problems:

- problem/incident and request management:
  - logging/raising of support requests
  - tracking of request progress
  - tracking open and closed tickets
- knowledge management:
  - identification of staff training needs (for example use of particular software)

Knowledge – What you need to teach

- collating of user support knowledge
- change management:
  - supporting implementation of new systems
- configuration/asset management:
  - tracking software licences
  - responding to requests for hardware and software
  - decommission or redeployment of systems/users
- methods used to identify and resolve user problems:
  - troubleshooting to diagnose problems:
    - information gathering:
      - investigation of support requests
      - investigation of probable causes
      - troubleshoot issues (for example check line speeds, check uptime and downtime)
    - problem analysis:
      - elimination of known fixes and problems
      - elimination of potential causes
      - consideration of remaining possibilities
    - test remaining possibilities:
      - testing and elimination of possible causes
      - identify the appropriate solution
    - problem resolution:
      - backing up data on system
      - implementing the solution
      - testing the solution
      - repeating the process until required outcome
  - documenting the cause and solution on content management system
  - implementing security controls to mitigate against cause reoccurring

K2.6 The types of end user devices and systems where content management systems can be applied to identify and resolve user problems:

- desktop:

Knowledge – What you need to teach

- thick clients
- thin clients

- cloud workspaces:
  - free cloud workspaces
  - paid licensed cloud workspaces
- mobile devices:
  - tablets
  - smartphones
  - wearable technology (for example smartwatches)
  - e-reader
- laptops
- peripherals:
  - mouse
  - keyboard
  - monitors
  - printers/scanners
  - speakers
  - projectors
  - storage drives
  - magnetic reader/chip reader
  - smart card reader
- IoT:
  - smart buildings:
    - alarm systems (for example fire, security)
    - metres (for example water, power)
    - lighting
  - smart devices:
    - autonomous vehicles
    - TVs

K2.7 Types of operating systems and how they are used in a digital support environment:

Knowledge – What you need to teach

- end user (for example Windows, macOS, Linux):
  - used on desktop PCs and laptops
- mobile (for example iOS, Android):
  - used on tablets, devices and mobile phones
- server (for example Windows, Linux):
  - used in client-server network environments

K2.8 The range of application types used in a digital support context:

- productivity software:
  - word processing software
  - spreadsheet software
  - presentation software
  - visual diagramming software
- web browser
- collaboration software:
  - email client
  - conferencing software
  - voice over internet protocol (VoIP)
  - instant messaging software
  - online workspace
  - document sharing
- business software:
  - database software
  - project management software
  - business-specific applications (bespoke)
  - accounting software
  - customer relationship management (CRM)
  - ticket management software
- development software:
  - computer-aided design (CAD)
  - integrated development environment (IDE)

Knowledge – What you need to teach

K2.9 Application installation and configuration concepts in a digital support context:

- system requirements:
  - storage space
  - RAM
  - compatibility
  - processor
  - OS
- hardware configuration:
  - hard disk drive (HDD) configuration:
    - advantages:
      - increased storage capacity
      - lower cost
    - disadvantages:
      - high risk of damage due to moving parts
      - greater potential to overheat
  - solid state drive (SSD) configuration:
    - advantages:
      - faster access
      - faster write and rewrite speeds
      - lower risk of damage due to no moving parts
      - applied in devices to reduce device size (for example mobile phone, tablet)
    - disadvantages:
      - higher cost
      - less storage capacity
  - network card configuration:
    - advantages:
      - efficiency
      - highly secure
      - runs efficiently
    - disadvantages:

Knowledge – What you need to teach

- higher cost
- performance lifespan

- resource setup for performance optimisation
- permissions:
  - folder/file access for installation and operation
  - user authorisation
  - principle of least privilege
- security considerations:
  - impact to device
  - impact to network
  - impact on usability
  - impact on the way data is stored

K2.10 Operating system (OS) deployment considerations in a digital support context:

- system requirements
- hardware configuration
- methods of installation and deployment:
  - network-based
  - local (for example CD/USB)
  - virtualised
  - cloud-based
- boot methods:
  - internal hard drive:
    - SSD
    - HDD
  - external media drive:
    - optical media
    - USB-based/solid state (for example flash drive, hot-swappable drive)
  - network-based:
    - preboot execution environment (PXE)
    - Netboot

Knowledge – What you need to teach

- partitioning:
  - dynamic
  - basic
  - primary
  - extended
  - logical
  - GUID partition table (GPT)
- file system types:
  - extensible file allocation table (exFAT)
  - FAT32
  - new technology file system (NTFS)
  - resilient file system (ReFS)
  - compact disc file system (CDFS)
  - network file system (NFS)
  - third extended file system (ext3)
  - fourth extended file system (ext4)
  - hierarchical file system (HFS)
- file system formatting:
  - quick format:
    - files easier to recover
    - no scanning for bad sectors
    - less time intensive
  - full format:
    - full scrubbing of files
    - files harder to recover
    - full scan of bad sectors
    - more time intensive

K2.11 The types of deployment methods and the advantages and disadvantages of their application:

- unattended installation – requires minimal technician response due to pre-defined options being set up:

Knowledge – What you need to teach

- thin imaging:
  - advantages:
    - used on a large scale
    - used on a variety of devices
    - ability to put out latest software for build
    - flexibility
  - disadvantages:
    - requires more maintenance
    - more difficult to configure
- base image:
  - advantages:
    - used on a large scale
    - built to meet specific purpose
    - easier to create
  - disadvantages:
    - more difficult to maintain
    - less flexible

- in-place upgrade – upgrading an operating system without a full clean install
  - advantages:
    - efficient process
    - user profiles are not lost
    - simple process
  - disadvantages:
    - potential compatibility issues
    - requires operating system media or large download
- manual clean install – installing an operating system with the installation media
  - advantages:
    - most appropriate/latest version of operating system
    - simple process
  - disadvantages:

Knowledge – What you need to teach

        - may require a back-up
        - timely process
    - repair installation – performing a repair installation without data loss and without upgrading
        - advantages:
            - no loss of data
            - no need to check compatibility
            - may resolve operating system and application instabilities
        - disadvantages:
            - manual process
            - may not resolve operating system and application instabilities
    - multi-boot – ability to boot a single device with multiple operating systems
        - advantages:
            - ability to run multiple operating systems from different manufacturers
        - disadvantage:
            - difficult to set up and maintain
    - remote network installation – installing an operating system from a network boot
        - advantages:
            - physical access may not be needed
            - takes advantage of unattended installation
            - efficient deployment to multiple devices
        - disadvantages:
            - speed of deployment is limited to network capabilities
            - specific network configuration may be required
            - requirement for specific device features (for example PXE booting capabilities)
            - significant configuration required

K2.12 The steps in creating and deploying disk images:

- creation of a base image file
- creation of customisation or answer file
- addition of any additional drivers and software required
- distribution of the image

Knowledge – What you need to teach

- deployment of the image
- updating software versions and drivers to avoid introducing vulnerabilities and instabilities

K2.13 The benefits of using image files to deploy operating systems or software:

- automation requires fewer resources
- ensures consistency of deployment
- reduces ongoing support costs
- quick system restoration

K2.14 The purpose and process of system recovery and restoration:

- system recovery:
  - fixes a system in its current state
  - preserves all files and folders
- system restoration:
  - applied when system recovery fails
  - reverts system back to a previous state
- process:
  - ensuring data is backed up
  - booting in system recovery tools
  - following on-screen instructions
  - testing of issue to confirm resolution

K2.15 The purpose and types of corporate and internet service provider (ISP) email configurations and their applications within digital support:

- email configuration – server configuration of an email account used when traffic moves through a firewall or when configuring an email account set-up:
  - post office protocol 3 (POP3) – used to receive emails from the server to a local piece of software
  - internet message access protocol (IMAP) – allows emails to be held on a mail server and received by software
  - simple mail transfer protocol (SMTP) – used to receive emails that are sent over the internet
  - secure/multipurpose internet mail extensions S/MIME) – used to send encrypted email messages
  - port and secure sockets layer (SSL) settings – encrypted connection between the website server and the browser to improve security
  - transport layer security (TLS) – successor to SSL, used to provide security for data

Knowledge – What you need to teach

K2.16 The process of the configuration of on-premise and cloud-based integrated commercial provider email services:

- ensuring alignment with corporate policy
- configure user profiles (for example usernames, passwords, email signatures)
- identifying and selecting:
  - provider (for example G Suite, Microsoft 365)
  - protocol (for example SMTP, IMAP, POP3)
  - configure mail exchange (MX) record
  - domain for incoming mail
  - domain for outgoing mail

K2.17 The purpose of remote access and its application within digital support:

- purpose:
  - facilitates work from a remote location using network resources as if connected to a physical network or a choice of multiple networks (for example facilitates working from home due to office closure as part of a BCP)
- applications:
  - desktop sharing
  - remote support (for example fault diagnosis, remote correction of user issues)
  - off-site working

K2.18 The role and configuration factors of a VPN in securing remote access and remote support to protect data:

- role:
  - encrypts network traffic
  - masks IP address to increase privacy
- configuration factors:
  - settings
  - client configurations
  - server configurations
  - port and security protocols (for example TLS, SSL)
  - encryption setting and certificates
  - authentication

Knowledge – What you need to teach

K2.19 The process of configuring a simple VPN:

- configuration of the VPN server:
  - enabling the VPN service
  - configuring IP address and DNS hostnames of the VPN interface
  - managing user access including authentication and permissions
- configuration of the client device:
  - creating the connection
  - setting the destination IP address and fully qualified domain name (FQDN)
  - setting permissions and conditions

K2.20 The support processes provided to end users and customers:

- user management:
  - adding users
  - removing users
  - accessing times
- password management:
  - complexity setting
  - expiry
  - reset on next logon
- permissions and privileges:
  - access to resources
  - group policies
  - configuring shared resources
- installation and deployment of software
- connection to remote resources
- fault identification
- issue escalation from 1st to 3rd line support
- knowledge management:
  - documentation
  - known fixes
  - SOPs

Knowledge – What you need to teach

- asset management
- auditing

K2.21 The components of version control management and its application within digital support:

- fresh installation:
  - OS
  - application software
  - utility software
  - licensing
- patching and updating:
  - system updates (for example OS updates)
  - driver/firmware updates
  - anti-virus/anti-malware updates
  - software and applications
- updates:
  - installation of updates
  - roll back procedures:
    - roll back device drivers
  - roll back OS update failures
  - roll back updates
- deployment using network tools (for example group policy):
  - locally installed
  - network deployed
  - testing
  - release control

K2.22 The process of asset management and its application in digital support:

- identification and planning:
  - user needs
  - organisational needs
  - constraints
  - deployment strategies

Knowledge – What you need to teach

- acquisition and implementation:
  - sourcing assets (for example hardware and software)
  - integration into current system
- operation and maintenance:
  - tracking software licences
  - responding to requests for hardware and software
- decommissioning and redeployment:
  - removing non-utilised assets
  - decommissioning out-of-date systems
  - management of new or leaving staff profiles

K2.23 The purpose and applications of mobile device management (MDM):

- purpose:
  - tracks and locates mobile devices
  - secures mobile devices
  - manages use of devices
  - manages configurations:
    - wireless data network
    - cellular data network
    - hotspot
    - tethering
    - airplane mode
    - Bluetooth
    - email accounts
- applications:
  - segregation:
    - multiple profile options for personal and professional use
    - management of application data
    - compliance with organisational policies and procedures
  - remote management:
    - remote wipe

Knowledge – What you need to teach

        - disabling functionalities
        - restricts mobile devices
        - controls app store
        - restricts calling/data use
        - controls back-up and synchronisation
    - security:
        - screen lock
        - encrypts device
        - password enforcement
        - failed login attempts/login restrictions
        - multi-factor authentication
        - authenticator applications (for example Google authentication, fast identity online (FIDO))

K2.24 The methods and tools used to train others in using digital systems and technologies, and the appropriate applications of these methods and tools:

- methods:
    - shadowing
    - desk side
    - remote support
    - e-learning
    - VR
    - AR
    - smart boards
    - applications (for example Kahoot!, Padlet)
    - simulation
- tools:
    - crib sheets
    - smart sheets
    - webinars
    - screencasts
    - managed learning environments (MLE)

Knowledge – What you need to teach

- virtual learning environments (VLE)
- sandboxed environments
- MOOCs

Skills – What you need to teach

The student must be able to:

S2.1 Install and configure software and systems onto end user devices:

- remotely install an operating system and configure system settings:
  - select appropriate boot drive and configure with the correct partitions/formats
  - configure domain set-up
  - configure time, date, region and language settings
  - install additional drivers
  - install any available updates (for example Windows updates)
- upgrade an existing operating system ensuring all user data is preserved
- install productivity software:
  - apply software updates
- install network-based software

(GDC1, GDC6)

S2.2 Monitor and operate information systems:

- analyse performance of system components:
  - hardware
  - software
  - database
  - network
  - people
- assess and monitor the appropriate security controls (for example firewalls, anti-virus)
- monitor network performance and user traffic
- operate and maintain assets:

Skills – What you need to teach

- track software licences
- respond to requests for hardware and software
- log and tag assets correctly

- support users via face-to-face or remote access software:
  - train users in use of the system
  - organise and record user issues within a content management system
  - user password management
  - fault identification
  - issue escalation
- record and summarise all relevant findings and actions to inform future policies and procedures:
  - logically organise all findings
  - using appropriate technical terms

(GEC1, GEC4, GMC2, GMC3, GMC5, GDC1, GDC3, GDC6)

S2.3 Solve problems as they arise and apply appropriate methods in a digital support context:

- apply troubleshooting to diagnose problems:
  - information:
    - investigate support requests
    - investigate probable causes
    - troubleshoot issues
  - problem analysis:
    - eliminate known fixes and problems
    - eliminate potential causes
    - consider remaining possibilities
  - test remaining possibilities:
    - test and eliminate possible causes
    - identify the appropriate solution
  - apply problem resolution:
    - back-up data on system
    - implement the solution
    - test the solution

Skills – What you need to teach

- repeat process until required outcome is achieved
- document the cause and solution on fault logging system
- implement actions to mitigate against the cause reoccurring

S2.4 Deploy software applications and operating systems remotely:

- gather and analyse user data to determine requirements
- select and configure appropriate deployment method:
  - thin imaging:
    - gather software installer and drivers and build task sequence
  - base image:
    - install operating systems, drivers and software
    - configure operating system, applications and drivers
    - capture disk image
- deploy operating system with chosen method
- apply updates to operating system, applications and drivers
- test deployment meets business requirements
- comply with organisational safety and security policies and procedures

(GDC3, GDC4, GDC5)

S2.5 Configure accessories and ports of mobile devices for network connectivity:

- apply mobile device management (MDM) to configure mobile devices to allow:
  - wireless data networks
  - cellular data networks
  - hotspots
  - tethering
  - airplane mode
  - Bluetooth
  - email accounts

(GDC6)

S2.6 Explain the application and benefits of digital solutions to meet specific requirements:

- analyse requirements:
  - access to information, services or products

Skills – What you need to teach

- conducting transactions

- identify the best application of digital solutions to meet requirements:
  - digital systems (for example content management systems)
  - productivity software
  - digital technologies
- explain the benefits of applying the identified digital solution:
  - express ideas clearly and concisely
  - use appropriate level of detail to reflect audience requirements
  - use technical terminology

(GEC1, GEC3, GEC4, GMC10, GDC4)

S2.7 Operate digital information systems and tools to maintain information and delivery of a digital support service:

- operate information systems to collect, store, maintain and distribute information to support service delivery
- process and review user feedback data on service:
  - critically analyse validity of user feedback
- maintain service delivery and information:
  - create, action and update tickets
  - communicate the status of tickets with users
  - monitor and record system performance
  - support users remotely by utilising remote support software
- record and summarise all relevant findings and actions to inform future policies and procedures:
  - logically organise all findings
  - using appropriate technical terms

(GEC1, GEC4, GEC6, GMC5, GMC6, GDC3, GDC4)

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach

The student must understand:

K3.1 Types of sources of knowledge that can be applied within digital support:

- academic publications (for example textbooks, research journals and periodicals)
- supplier literature (for example handbooks or online articles for specific devices, computers or laptops)
- search engines (for example Google, Bing)
- websites (for example wikis, forums, Stack Overflow, manufacturers' websites)
- social media (for example company profiles for Twitter, Facebook and LinkedIn)
- blogs (for example reviews of new technologies, opinions on topical issues in the digital sector)
- vlogs (for example demonstrations, tutorials on digital technologies)
- professional networks (for example digital transformation networking events/conferences)
- e-learning (for example MOOCs, recognised vendor qualifications, Cisco)
- peers (for example colleagues, network contacts, other industry professionals)

K3.2 The factors of reliability and validity to be applied to legitimise the use of sources of knowledge:

- industry-certified accreditation (for example Cisco certified network associate (CCNA1), Microsoft technology associate (MTA), network fundamentals)
- appropriateness
- evidence-based:
  - citations
- relevant context
- credibility of author:
  - affiliated to specific bodies (for example government, industry regulators)
  - reputation
  - experience (for example relevant qualification in subject)
- target audience – produced with specific audience requirements taken into consideration (for example use of technical/non-technical terminology)
- publication:
  - version (for example use of the current version)
  - date of publication (for example if the content is outdated)

Knowledge – What you need to teach

K3.3 The factors of bias:

- types of conscious and unconscious bias:
  - author/propriety bias – unweighted opinions of the author or owner
  - confirmation bias – sources support a predetermined assumption
  - selection bias – selection of sources that meets specific criteria
  - cultural bias – implicit assumptions based on societal norms
- indicators of bias within sources:
  - partiality
  - prejudice
  - omission
- bias reduction:
  - based on fact/evidence
  - inclusive approach:
  - full representation of demographics
  - objectivity

K3.4 Process of critical thinking and the application of evaluation techniques and tools:

- process of critical thinking:
  - identification of relevant information:
    - different arguments, views and opinions
  - analysis of identified information:
    - identify types of bias and objectivity
    - understand links between information and data
  - selection of relevant evaluation techniques and tools
  - evaluation of findings and drawing of conclusions
  - recording of conclusions
- evaluation techniques:
  - formative evaluation
  - summative evaluation
  - qualitative (for example interviews, observations, workshops)
  - quantitative (for example experiments, surveys, statistical analysis)

Knowledge – What you need to teach

- benchmarking
- corroboration:
  - cross-referencing
- triangulation

- evaluation tools:
  - gap analysis
  - KPI analysis
  - score cards
  - observation reports
  - user diaries
  - scenario mapping
  - self-assessment frameworks
  - maturity assessments

K3.5 The functions of incident and request management systems in communicating information:

- reporting:
  - ticket-based:
    - users log issue via ticket system or email
    - digital support manually input details if user contacts via telephone
    - tracks issue trends
    - records internal customer satisfaction
  - online chat bots:
    - artificial intelligence (AI) responds to commonly asked questions
    - efficient use of digital support resource
- recording requirements:
  - user/customer details
  - issue details
  - resolution
  - time taken
- tracking and communicating progress:
  - visibility on status and escalation

Knowledge – What you need to teach

K3.6 Methods of communication and sharing knowledge and their application within a digital support context:

- integrated and standalone IT service management tools:
  - incident and problem management systems
  - change management systems
- knowledge bases and knowledge management systems
- wikis and shared documents
- shared digital workspaces
- telephone
- instant messaging
- email
- video conferencing
- digital signage
- social media:
  - organisational
  - public
  - personal
- blogs
- community forums
- project management tools (for example issue logs, Gantt charts, Kanban boards, burndown charts)
- policy, process and procedure documents

Skills – What you need to teach

The student must be able to:

S3.1 Identify sources of knowledge and apply factors that legitimise their use to meet requirements in a digital support context:

- identify and clarify the parameters of the requirements
- identify appropriate sources of knowledge (up to 3) (for example search engines, blogs)

Skills – What you need to teach

- apply the factors of reliability and validity to identified sources (for example authority, date of publication)
- assess and review potential bias of sources
- assess and review the identified sources' appropriateness to meet the requirements

(GEC4, GDC1)

S3.2 Search for information to support a topic or scenarios within digital support and corroborate information across multiple sources:

- identify and clarify the parameters of the search (for example explore the future of the digital economy, identify trends in big data)
- identify the sources of data that contain the required information
- safely and securely search sources for the information required
- corroborate sources by applying cross-referencing across multiple sources
- apply reliability and validity factors
- assess and review potential bias of sources

(GEC4, GDC5)

S3.3 Select and apply techniques and tools to support evaluation in a digital support context:

- identify and clarify the parameters of the evaluation
- select appropriate techniques and tools to support the evaluation
- apply the selected techniques and use the appropriate tools to support the evaluation
- record the findings of the evaluation for the requirement

(GEC4, GDC2)

S3.4 Compare options of sources and rationalise the actions taken to ensure the reliability and validity of sources:

- identify the sources for comparison
- apply the relevant reliability and validity factors to the sources
- compare the outcomes of the validity and reliability actions
- explain and recommend the choice of action to ensure the sources are reliable and valid, using appropriate technical terms

(GEC1, GEC3, GEC5, GMC5, GDC3)

S3.5 Identify and understand bias when using sources of knowledge in a specific digital support context:

- identify the types of bias (for example confirmation, unconscious)

Skills – What you need to teach

• identify the indicators of bias within the source
• explain clearly and concisely how bias has been created within the source
• explain clearly and concisely how bias can be avoided within sources
(GEC1, GEC3, GEC5, GMC6, GDC3)
S3.6 Demonstrate critical thinking within a digital support context:
• apply the process of critical thinking to meet requirements
  ○ identify relevant information
  ○ analyse the information
  ○ select and apply appropriate evaluation techniques and tools
  ○ evaluate findings
  ○ logically organise and record conclusions
(GEC1, GEC3, GMC5, GMC6, GMC8, GDC3, GDC4)

Occupational specialism: Cyber Security

The numbering is sequential throughout the performance outcome, from the first knowledge statement, following on through the skills statements. The ‘K’ and ‘S’ indicate whether the statement belongs to knowledge or skills.

Mandatory content

- Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data
- Performance outcome 2: Propose remediation advice for a security risk assessment
- Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Performance outcome 1: Apply procedures and controls to maintain the digital security of an organisation and its data

Knowledge – What you need to teach

The student must understand:

K1.1 The purpose of organisational information security governance:

- to investigate, control, communicate and report cyber risks
- to provide a security framework for:
  - defined roles and responsibilities (for example, data controller and data processor)
  - organisational policies and processes (for example, data retention and deletion)
  - outlining security activities (for example, evaluation of new systems and technologies)
- to manage compliance against legislation, frameworks and standards (for example, ISO27001, data protection, freedom of information (FOI) requests)
- to align organisational priorities and operations to mitigate against cyber threats and vulnerabilities (for example, company password complexity requirements)

K1.2 The application of IT governance principles in an information security context:

- responsibility – all staff involved in information security will understand their specific roles and responsibilities (for example, asset owner, data controller and data processor)
- strategy – strategies need to be secure by design, taking into account information security constraints and future infrastructure requirements (for example, cloud-based services and data sharing) based on business requirements
- acquisition – all purchases are evaluated, taking into account risks, benefits and costs to ensure appropriate ongoing analysis of information security and transparent decision making
- performance – the necessary levels of preventative and remediative performance are in place to guarantee the confidentiality, integrity and availability of the information

Knowledge – What you need to teach

- conformance – IT, data and information are used in accordance with all mandatory and relevant information security legislation and regulations
- human behaviour – technical and non-technical controls are considered in policies, processes and decisions to maintain information security

K1.3 The types and application of cyber security protection methods utilised in network infrastructure and system software:

- hardware:
  - hardware protection – the use of server and software solutions to protect hardware and data
  - device hardening – the application of updates and secure configurations to a device to increase security
  - physical controls – storing hardware in secure locations, in locked cages and/or in areas with CCTV and key card access-controlled doors
- operating systems (OS):
  - installation of updates or patches – the application of updates correcting security issues in older versions of the software:
    - roll back – use of a system snapshot to aid recovery from unforeseen issues with patches or updates
  - OS hardening – the removal of unnecessary accounts, functions, applications, ports and access through the application of security policies to minimise exposure to current and future threats
- networks:
  - segmentation and isolation – the separation of network, systems, data, devices and services to limit the ability for threat actors to traverse the network
  - network monitoring – the use of tools to monitor and analyse network traffic to prevent potential threats and attacks
  - network hardening – the securing of communication channels and systems between servers and devices on a shared network
  - firewalls – the control and monitoring of access into and out of networks
- software:
  - anti-malware and anti-virus – to protect against malicious software
  - authentication methods:
    - single sign-on (SSO) – the use of one set of credentials to login to multiple services and the ability to easily manage access and control multiple systems

Knowledge – What you need to teach

        - multi-factor authentication (MFA) – the use of 2 or more factors to achieve authentication – something you know (for example, password), something you have (for example, token) and something you are (for example, biometric)
    - remote monitoring and management (RMM) – the remote management of devices and performance of tasks including auditing, installing, upgrading or removing software, and obtaining diagnostic information
    - vulnerability management and scanning – the use of an automated process to manage and identify security vulnerabilities in software infrastructure
    - application hardening – the protection for an application against unauthorised access by eliminating vulnerabilities and increasing layers of security
    - access controls – the assignment and management of access to information:
        - credentials – ensuring that passwords conform to a strong password policy of sufficient length and complexity and that users are trained on how to protect their password
        - privileged access management (PAM) – a security measure used to control and monitor privileged users' activity
    - application firewalls – the control and monitoring of access and data in and out of applications
    - patching – ensuring that the latest security patches for installed software have been applied
- cloud:
    - auditing and monitoring – detection of unauthorised or unusual behaviour through reviewing logs
    - access controls – the assignment and management of access to information
    - MFA – the use of 2 or more factors to achieve authentication, such as something you know (for example, password), something you have (for example, token), something you are (for example, biometric) and somewhere you are (for example, IP address location)

K1.4 The potential applications of cyber security principles in network infrastructure design:

- establish the context before designing a system:
    - adapting a zero-trust approach at an early stage to ensure all network access requires verification
    - establishing the system's purpose, any requirements for operation, and what is deemed an acceptable risk
    - identifying the potential vulnerabilities that affect the system
    - considering end user behaviours and development of use cases as required
    - defining any supplier's role in establishing and maintaining system security
    - identifying organisation infrastructure from end to end, taking into account the sensitivity of data and where it is stored, manipulated and rendered

Knowledge – What you need to teach

- clarifying the governance of security risks and ensuring there is no ambiguity about roles and responsibilities of those involved in designing and operating a system

- make compromise difficult:
  - transforming, validating, and rendering data to obscure or anonymise information
  - reduction of the attack surface to reduce potential points of entry
  - having relevant security controls in place that are regularly reviewed and tested
  - ensuring all management and operational environments are protected from targeted attacks
  - applying reliable and tested solutions in line with industry and organisational best practice
  - authorising and accounting for all individual operations through auditing and change control
  - designing networks and infrastructure for efficient maintenance and management (for example, access control, security patching)
- make disruption difficult:
  - ensuring systems are resilient to both attack and failure
  - designing networks and infrastructure for scalability to handle sudden and increased demand
  - identifying any potential bottlenecks that could be exploited by high load and denial of service conditions
  - identifying where availability depends on a third party and planning for the failure of that third party
  - carrying out regular testing by performing mock incident/event response scenarios to simulate a real attack
  - making it challenging for attackers to detect security rules via external penetration testing
- make compromise detection easier:
  - gathering and analysing relevant security incident/event information and logs to identify unauthorised actions
  - ensuring alerts are in place to identify and detect known malware and to control communications
  - ensuring separation of monitoring and operational systems to allow alerting and logging to remain operational during a cyber incident/event
  - regular monitoring to understand normal behaviours, making abnormal behaviours easier to detect
- reduce impact of compromise:
  - making use of network segmentation to limit movement of malware or threat actors across the network
  - removal of unnecessary functionality, queries or caches of data which could be compromised

Knowledge – What you need to teach

- avoiding the creation of a management bypass which could be used by threat actors to bypass security controls
- ensuring the recovery process is straightforward and tested regularly
- designing the network to support a separation of duties to ensure no individual or account can create a cyber incident/event either intentionally or unintentionally
- anonymisation of data to prevent the potential loss of personal information

K1.5 The types and functions of operating systems and key components to support cyber security investigations:

- operating systems and devices to support them:
  - client side (for example, Windows, macOS, Linux) – devices include desktop PCs and laptops
  - mobile (for example, Android, iOS) – devices include tablets and mobile devices
  - server side (for example, Windows, Linux) – a network operating system installed on a server
- functions of operating systems:
  - security – implements restrictions and controls to protect data and software (for example, zero trust)
  - system performance – provides an interface between software and hardware to enable efficient performance
  - error detection – detects issues and abnormalities with system software and hardware
  - graphical user interface (GUI) – provides an interface for users to interact with the device
  - memory management – controls operating systems' memory allocation and prevents applications reading other applications' memory
  - processor management – security controls are implemented within the processor to provide additional protection (for example, protection against side-channel attacks)
  - device management – the operating system may implement security controls when interfacing with hardware (for example, requiring signed drivers)
  - file management – enables the operating system to manage data storage and retrieval
  - program execution – enables the operating system to control how and when users can execute code and programs, and with what level of permission and access those applications have
  - handling input/output operations – the operating system is responsible for processing user input (for example, keystrokes on a keyboard) and output (for example, graphics on a screen)
- key components for cyber security investigation:
  - configuration files – stored in one location on a Linux system each containing settings and instructions for applications and processes

Knowledge – What you need to teach

- registry – a database of configurations for a Microsoft Windows based system that manages values for installed hardware and software
- logs – used to monitor network performance and traffic flow
- library/preferences – stored in one location in MacOS, the system preference files contain rules for the system and applications
- file system – stores, manages and organises data on the storage disk – this can differ depending on the operating system (for example, NTFS, FAT32, exFAT, APFS, ext4)
- processes – provides real time information on a Microsoft Windows based system

K1.6 The role of physical and virtual server types:

- server (for example, Linux, Windows Server) – applied to client-server environments:
  - physical servers – running applications directly on physical hardware, allowing full access to the hardware
  - virtualisation:
    - virtual servers – allows a single piece of hardware to run multiple operating systems and software at the same time, in isolated environments
    - containers – virtualisation of software and application packages which are separated and isolated from other packages and the underlying operating system for added security and portability using only packages required for the software to function

K1.7 The purpose and core processes of IT service management (ITSM):

- purpose – to manage the end-to-end delivery of IT services to customers
- core processes:
  - service request management – handling queries from customers and tracking the resolution of incidents/events (for example, reporting of a potential cyber incident/event to the service desk)
  - knowledge management – maintaining documentation, ensuring it is up to date and relevant (for example, documented and standardised hardened builds)
  - IT asset management – using tools (for example, configuration management database (CMDB)) to keep track of hardware, software, systems and IT configurations (for example, history, location, owner)
  - problem and incident management – understanding the root causes and co-ordinating, responding to, and resolving incidents/events as they occur (for example, standardised incident management process and procedures in place for cyber incidents/events)
  - change management – ensuring that changes to IT services are agreed upon by stakeholders and recorded (for example, introduction of a new firewall rule)

Knowledge – What you need to teach

K1.8 The application of the Information Technology Infrastructure Library (ITIL®) service lifecycle:

- service strategy – aligns to business objectives to ensure that the service is fit for purpose and fit for use
- service design – design of services and all supporting elements for introduction into the live environment, ensuring that people, processes, products and partners are all considered
- service transition – building and deploying services and ensuring that any changes are managed in a coordinated way
- service operation – fulfilling requests, resolving failures, fixing problems and carrying out routine operational tasks
- continual service improvement – continually improving the effectiveness and efficiency of IT processes and services

K1.9 The application of cyber security principles associated with the transmission of digital information:

- identification of the security requirements of the data:
  - making use of the CIA triad – confidentiality, integrity and availability applied to develop security
- prevention of eavesdropping of data whilst in transit:
  - making use of asymmetric encryption techniques
- authentication and verification of data:
  - making use of aspects of cryptography – integrity, authenticity, confidentiality, non-repudiation

K1.10 The role of frameworks and standards to support an organisation's information security management system (ISMS):

- role of ISMS – used to create policies (for example, information security policy, acceptable use policy) to ensure an organisation is compliant with security and privacy standards
- role of frameworks:
  - Control Objectives for Information and Related Technologies (COBIT) – used in helping organisations to develop procedures and internal frameworks for governance and management of IT systems
  - Service Organisation Controls (SOC 2) – used in assessing an organisation's security, availability, processing integrity, confidentiality and privacy controls
  - National Institute of Standards and Technology (NIST) – used by organisations to help them understand ways to improve how they manage cyber security risks
- role of standards:
  - ISO 27000 information security management – a series of standards and best practice guides for information security management:

Knowledge – What you need to teach

        - ISO 27001 – used to establish, implement, maintain and continually improve an information security management system within an organisation
    - ISO 35800:2015 – a framework for governance of IT for an organisation
    - National Cyber Security Centre (NCSC) Cyber Essentials and Cyber Essentials Plus – a government backed scheme that supports organisations to protect against cyber attacks and provides accreditation to organisations
    - Payment Card Industry Data Security Standard (PCI DSS):
        - designed to reduce payment card fraud by increasing security controls for organisations that store, process or transmit credit card data

K1.11 The purpose and importance of a disaster recovery plan (DRP) to support risk management:

- purpose – a formal document that details instructions on how to respond to unplanned incidents/events, including natural disasters, power outages, cyber attacks and any other disruptive events
- importance:
    - minimises mean time to recovery (MTTR)
    - minimises interruptions to normal operations
    - limits the extent of disruption and damage
    - minimises the economic impact of the interruption
    - establishes alternative means of operation in advance
    - enables a prompt restoration of service
    - supports the identification of potential issues (for example, lack of staff training)

K1.12 The implementation of a DRP to support risk management:

- defining the scope of the incident/event:
    - environmental or technical impact – determining the nature of the disaster
    - organisational impact – identifying if the disaster impacts all users across the organisation
    - departmental impact – identifying how departments are impacted by the disaster
    - individual impact – identifying how individuals are impacted by the disaster
- gathering relevant information:
    - historic outage details
    - inventories of hardware, software, networks and data
    - contact information for any parties involved

Knowledge – What you need to teach

- risk-assessing – identifying threats and vulnerabilities in assets and determining the likelihood of occurrence and impact on business-as-usual operations
- creation of the plan:
  - identifying the resources required for the DRP:
    - systems, equipment and utilities required to continue business as usual operations
    - staff contact details and documented roles and responsibilities
    - financial commitment required to implement the DRP in response to incident/event
- plan approval:
  - sign off by appropriate parties
- testing of the plan:
  - identifying scope of the test and required resources
  - determining frequency of the test
  - conducting the test
  - reviewing and documenting outcome of the test
  - amending the plan based on review as required
- continuous improvement:
  - internal and external auditing of plan

K1.13 The purpose and types of preventative controls implemented to protect an organisation's information:

- purpose – to prevent unauthorised access or tampering, or mitigate against environmental incidents/events through the implementation of effective controls
- physical controls:
- specialist locks:
    - anti-picking
  - barriers:
    - fencing
    - bollards
    - gates
    - cages
  - flood and fire defence systems
- managed entry access controls:

Knowledge – What you need to teach

- manned reception desk
- security guards
- restricted door controls
- card readers
- biometric:
  - facial recognition
  - fingerprints
- video/closed-circuit television (CCTV)
- pin/passcodes

- technical controls:
  - firewalls
  - allow and deny control lists
  - sandboxing
  - device hardening:
    - changing default passwords
    - setting correct permissions on files and services
    - applying updates and fixes
    - removing unnecessary software
    - application of security policies
    - disabling unauthorised devices (for example, USB flash drives)
- procedural controls:
  - separation of duties and relevance of role-based access control (RBAC)

K1.14 The purpose and types of corrective controls implemented to protect an organisation's information:

- purpose – to limit the extent of damage and reoccurrence
- corrective control techniques:
  - physical controls:
    - fire suppression:
      - sprinklers
      - extinguishers

Knowledge – What you need to teach

        - gas suppression:
            - inert
            - chemical
    - technical controls:
        - patching
        - disconnecting infected systems
        - quarantining a virus
    - procedural:
        - standard operating procedure (SOP) (for example, actions taken when a fire is identified)
        - DRP

K1.15 The purpose and types of compensating controls implemented to protect an organisation's information:

- purpose – provides a safeguard against primary control failure
- compensating control techniques:
    - physical controls:
        - segregation of duties – sharing of responsibilities to ensure greater security measures are in place
        - log management and auditing (for example, key code access) – storing a log of which individuals enter a location
    - technical controls:
        - encryption
    - procedural controls:
        - mandatory and regular cyber awareness training
        - regular testing of controls (for example, simulated attacks)
        - SOPs (for example, environmental control monitoring)

K1.16 The purpose and characteristics of cryptography:

- purpose of cryptography – applying encryption or hashing to ensure the secure and authenticated transmission of data
- characteristics of cryptography:
    - encryption – reversible form of cryptography (for example, using public or private keys):
        - confidentiality – ensuring only the intended recipients of information can decrypt the data with symmetric or asymmetric encryption

Knowledge – What you need to teach

- authenticity – enables the recipient of data to verify the sender using digital signatures (asymmetric encryption)
- hashing – non-reversible form of cryptography using an algorithm to provide a fixed length output (for example, password hashing)
- integrity – ensures data cannot be modified in transit by utilising hash-based message authentication code (HMAC)

- non-repudiation – used in conjunction with other aspects of cryptography to provide a guarantee of the author of a message using a message authentication code (MAC)

K1.17 The purpose, features and types of digital certificates:

- purpose of digital certificates – an electronic signature that proves the authenticity of a device, server or user through the use of asymmetric cryptography
- features of digital certificates:
  - name of certificate holder – company, server, device
  - unique serial number – a unique number assigned only to one certificate
  - expiration date – the date after which the certificate is no longer valid
  - certificate holder's public key – used for encrypting and decrypting digital signatures and messages in association with public key infrastructure
  - issuers' signature – identification information of the issuing authority
- types of digital certificates:
  - server side – allows a client to verify the authenticity of a server
  - client side – allows a client to authenticate to a server
  - code signing – allows an operating system to verify the author and integrity of software

K1.18 The purpose of certificate management tools:

- monitors expiration dates
- revokes certificates, if required, before the expiration date
- performs auto renewal of expired certificates
- creates, signs and issues certificates:
  - auditing of certificates – validating a certificate is deployed/removed as required
  - diagnosis to confirm that appropriate certificates are deployed when resolving issues

K1.19 The process for the generation of a digital certificate:

- generation of a public and private key
- generation of a certificate signing request (CSR)

Knowledge – What you need to teach

- issuing and signing of certificate by a trusted certificate authority (CA)
- installation of certificate on client/server device

K1.20 The purpose of legislation in relation to the cyber security industry:

- Data Protection Act (DPA) 2018:
  - imposes obligations to:
    - protect personal data against cyber attacks
    - detect security events
    - minimise the impact of an incident/event
- Investigatory Powers Act 2016:
  - collates all powers of law enforcement, security and intelligence agencies to obtain information and data communications
  - updates the ways the investigatory powers are authorised and overseen
  - makes sure investigatory powers meet digital requirements
- Human Rights Act 1998:
  - protects human rights from exploitation
  - all public authorities or bodies exercising public functions must follow the act
- Telecommunications (Security) Act 2021:
  - introduces duties for providers of public electronic communications networks and services to:
    - prevent the occurrence of risks through identifying and reducing the chances of security compromises occurring
    - mitigate and remedy any effects in the event of a security compromise
    - inform network or service users of the security compromise
- Computer Misuse Act 1990:
  - criminalises the unauthorised interference with computers, including:
    - unauthorised access to computer material
    - unauthorised access to computer materials with intent to commit a further crime
    - unauthorised modification or deletion of data
    - making, supplying or obtaining anything that can be used in computer misuse offences
- Freedom of Information Act 2000:
  - protects certain security public authorities (for example, NCSC) and exempts them from having to disclose information

Knowledge – What you need to teach

- Network and Information Systems Regulations 2018 (UK):
  - aims to establish a common level of security for network and information systems
  - applies to 2 groups of organisations:
    - operators of essential services (OES)
    - relevant digital service providers (RDSPs)
- Official Secrets Act 1989:
  - protects the disclosure of information relating to security or intelligence
- Wireless Telegraphy Act 2006:
  - law relating to the regulation of wireless transmitting devices in the UK
  - aims to make it a criminal offence to obtain information from wireless networks without prior permission
  - prohibits the misuse of wireless technology (for example, intercepting and disclosing information)

K1.21 Key features of ethical codes of conduct within cyber security:

- UK Cyber Security Council Code of Ethics:
  - credibility:
    - maintain the highest standards in service delivery, advice and conduct
    - act in ways that are accountable and ethical
  - integrity:
    - show honesty and integrity in the conduct of activities and services
    - demonstrate compliance with legislation and regulations
  - professionalism:
    - uphold and improve the professionalism and reputation of the cyber security sector by sharing experiences, opportunities, techniques and tools
    - promote and advance public awareness and understanding of cyber security and its benefits
    - apply evidence-based practices
    - correct any false or misleading statements about the industry or profession
  - responsibility and respect:
    - take responsibility
    - demonstrate good practice with regards to the safeguarding of data and information
    - declare any conflicts of interest

Knowledge – What you need to teach

        - champion equality of opportunity, diversity and inclusion and support human rights, dignity and respect
- British Computer Society (BCS) code of conduct:
    - you make IT for everyone:
        - maintain professionalism whilst sharing information
    - show what you know, learn what you do not:
        - only undertake work within your professional competence
        - continuously develop your knowledge and skills
        - develop a good understanding of legislation
        - remain respectful and ethical
    - respect the organisation or individual you work for:
        - conduct duties demonstrating due care and diligence
        - show professional responsibility
        - do not disclose any information for personal gain
        - do not take advantage of the inexperience of others
    - keep IT real; keep IT professional; pass IT on:
        - uphold the reputation of the profession
        - help to improve professional standards
        - act with integrity and respect
        - encourage and support members

K1.22 The definitions of core terminology in cyber security:

- CIA triad – a model that forms the basis for security systems and consists of 3 core components:
    - confidentiality – the access and modification of data is restricted to authorised users
    - integrity – data is maintained in appropriate form without unauthorised modification
    - availability – authorised users are able to access data as required
- IAAA – a concept to explain access control in cyber security:
    - identification – a unique form of identity bespoke to the individual user (for example, full name, username, employee number)
    - authentication – the process of verifying a person's identity:
        - methods of authentication:
            - single factor authentication

Knowledge – What you need to teach

- MFA
- authorisation – the process of attributing and allowing permissions for users through access control models
- accountability – assurance of actions being performed by a user are traceable to confirm sender identify and proof of receipt

- access controls methods – restricts or allows access to areas of a business (for example, mandatory access control (MAC))
- defence in depth – the process of layering security mechanisms to provide protection to a system should one layer fail or be bypassed
- reliability – a system or component capability to function under specified conditions for a specified period of time
- assurance – analysis of security requirements of IT systems, policies and procedures to confirm that security requirements have been met

Skills – What you need to teach

The student must be able to:

S1.1 Apply and monitor procedures and security controls in the installation, configuration and support of physical or virtual infrastructure to ensure confidentiality, integrity and availability:

- set up a workgroup environment to include:
  - clients – minimum of 2
  - server
  - networking device – router or switch
- apply groups and roles within directory services
- set up, configure and distribute a certificate authority (CA)
- apply and monitor security controls according to NCSC Cyber Essentials:
  - boundary firewalls and internet gateways
  - secure configuration
  - malware protection
  - security update management
- apply and monitor appropriate access control methods to support physical or virtual infrastructure as required:

Skills – What you need to teach

- mandatory access control (MAC) – restrict or allow access based on a hierarchy of security levels
- discretionary access control (DAC) – restrict or allow access based on resource owner preference
- attribute-based access control (ABAC) – restrict or allow access based on attributes or characteristics
- role-based access control (RBAC) – restrict or allow access to resources based on the role of a user
- rule-based access control (RuBAC) – use a rule list to define access parameters

- manage physical and electronic documents and data accurately in accordance with data protection legislation

S1.2 Protect personal, physical and environmental security:

- review the potential security risk:
  - gather information from systems and users (for example, security events, logs)
- select and apply appropriate security controls in accordance with the risk:
  - preventative controls
  - corrective controls
  - compensating controls
- comply with relevant regulatory and organisational policies and procedures as required (for example, Data Protection Act 2018, data protection policy)

S1.3 Install and configure software used to identify and mitigate vulnerabilities on networks and end user devices (for example, servers, desktop computers):

- install and configure software to secure a network:
  - vulnerability scanning
  - anti-malware and anti-virus
  - firewall
- harden devices:
  - change default passwords
  - set correct permissions on files and services
  - apply updates and fixes
  - remove unnecessary software
  - apply security policies

Skills – What you need to teach

- disable unauthorised devices
- test that the installation and configuration of end user devices has been successful

(GDC1, GDC5, GDC6)

S1.4 Conduct a security risk assessment on a device connected to a local area network (LAN):

- identify risks
- assess the risk:
  - likelihood of a risk happening
  - severity of an incident/event
  - calculation of the overall security risk rating:
    - likelihood x severity = risk/RAG rating
  - asset value versus the potential mitigation controls
- recommend control measures to mitigate the risk:
  - considering usability and security
- record and summarise all relevant findings and actions, clearly and concisely, using appropriate terminology

(GEC3, GEC4, GMC5, GMC6, GMC8)

S1.5 Apply the process of continuous improvement to maintain the digital security of an organisation and its data:

- review existing control measures through a gap analysis:
  - identify changes that have occurred since controls were implemented
  - identify any missing requirements
- assess effectiveness of existing controls
- identify areas and required adaptions for continuous improvement to mitigate vulnerabilities (for example, an incident detected in networked equipment, updating devices with the latest releases of security software, penetrating testing)
- record and communicate suggested areas for continuous improvement

(GMC10, GDC3)

S1.6 Manage and assess the validity of security requests:

- assess the validity of the security request, considering:
  - origin of request
  - reason for request

Skills – What you need to teach
○ status and permissions of requestor (for example, staff member, external stakeholder) ○ sensitivity of request (for example, exposure of personal data) ○ any new risks that will be introduced as a result of the security request • manage security request in line with regulatory requirements (GDC4)

Performance outcome 2: Propose remediation advice for a security risk assessment

Knowledge – What you need to teach
The student must understand: **K2.1 The purpose and application of compliance principles in computer forensics:** • purpose: ○ a method of investigating and analysing digital devices and computer networks to gather legitimate evidence for presentation to an appropriate body (for example, law enforcement) • application of compliance principles: ○ identification – identification of what evidence is present and where and how it is stored ○ preservation – avoidance of tampering and contaminating evidence, either accidentally or intentionally, by isolating, securing and preserving digital evidence in a chronological order in line with legal retention periods ○ analysis – reconstructing fragments of data and drawing conclusions based on evidence ○ documentation – recording of all visible data and documentation of the investigation ○ presentation – presentation of all findings to an appropriate body (for example, law enforcement) for further investigation **K2.2 Types of potential cyber security threats and methods of identification:** • social engineering: ○ phishing – a fraudulent message designed to trick large numbers of individuals into revealing sensitive information or to deploy malicious software: ▪ message may be sent from a public email domain or a spoofed email address ▪ the domain name may be misspelt ▪ the email may be poorly written or contain spelling mistakes

Knowledge – What you need to teach

        - the email may include infected attachments or suspicious links
        - the message may create a sense of urgency
    - spear phishing – a difficult to detect, targeted email attack sent to specific individuals to trick them into clicking or downloading malicious software or initiating an undesired action (for example, bank transfer):
        - identification methods are similar to phishing but, as the attack is more sophisticated and personalised, it is more difficult to detect
    - vishing – fraudulent phone calls or voice messages purporting to be from reputable companies to induce individuals to reveal personal information:
        - may request confidential information (for example, date of birth, credit card numbers, National Insurance number)
        - may use a demanding tone to push victims to reveal information (for example, a memorable word used as part of multi-factor authentication (MFA))
        - call may be unexpected and unplanned (for example, claiming to be from a governmental department such as HMRC)
    - smishing – fraudulent text messages posing to be from reputable companies trying to persuade individuals to reveal personal information:
        - use of unknown or hidden numbers
        - message may appear to come from a well-known institution (for example, a bank requesting personal or financial information)
        - may include suspicious links (for example, offering a rebate or a refund)
    - shoulder surfing – criminal practice using observation techniques to get information (for example, pin numbers, passwords or other personal data):
        - individuals standing too close or looking over someone's shoulder
    - dumpster diving – a technique used to retrieve information from disposed items that could be used to carry out an attack:
        - use of discarded personal information
- denial-of-service (DoS) – a malicious attempt to overwhelm an online service and render it unusable:
    - identification through monitoring and analysis of network traffic:
        - degraded network performance
        - increased traffic to network
        - multiple requests from same IP address
        - service outages/website inaccessible

Knowledge – What you need to teach

- distributed denial-of-service (DDoS) – involves many computers attacking the same online service at the same time to render it unusable:
  - identification through monitoring and analysis of network traffic:
    - degraded network performance
    - increased traffic to network
    - multiple requests from same IP address
    - service outages/website inaccessible
- zero-day attack – exploited by the attacker before the developer can release a patch:
  - identification through monitoring and analysis of network traffic:
    - statistics provided by anti-malware vendors
    - unusual scanning activity
    - monitoring digital signatures using machine learning to identify previous attacks
    - monitoring interaction with existing software and systems to identify and manage malicious activity
- malware:
  - virus – spreads between networked devices and causes damage to data and software:
    - appearance on scanning reports
    - potentially reduced or inhibited performance of device
  - adware – unwanted programme that displays ads on computers and mobile devices:
    - unexpected change in web browser home page
    - web pages not displaying correctly
    - slow device performance
    - device crashing
    - reduced internet speeds
    - redirected internet searches
  - ransomware – malicious software designed to block access, delete or amend a computer system or data until a sum of money is paid:
    - inaccessible data
    - appearance on malware detection reports
    - user alerts

Knowledge – What you need to teach

- trojan – downloads onto a computer disguised as a legitimate programme or hidden within an application:
  - appearance on scanning reports
  - potentially reduced or inhibited performance of device
- botnet – network of computers or internet-connected devices under a threat actor's control:
  - slow internet access
  - device crashing
  - problems with shutting devices down
- spyware – hides on devices, monitors activity and steals sensitive information (for example, bank details, passwords):
  - appearance on scanning reports
  - potentially reduced or inhibited performance of device

- password attack – attempts by threat actors to determine a password:
  - brute force – a computer programme that works through all possible letter, number and symbol sequences character by character, until hitting the correct combination:
    - increased network activity
    - failed login attempts from the same IP address
    - unusual user behaviour
  - dictionary attack – a computer programme that uses common words and phrases to work out a password:
    - increased network activity
    - failed login attempts from the same IP address
    - unusual user behaviour
- man-in-the-middle – attackers attempting to intercept communications:
  - web browser security warnings
  - unexpected or repeated disconnections

K2.3 Types of threat actors and motivations for an attack, and the importance of threat intelligence:

- threat actors – a person, group or entity that performs a cyber attack:
  - cyber criminals – use of ransomware, social engineering or malicious software to steal sensitive information to result in financial gain
  - insiders – current or past employees use authorised access to gain company information to seek revenge or financial gain

Knowledge – What you need to teach

- terrorist organisations – cause disruption to organisations to bring awareness to their cause (for example, recruitment purposes, propaganda, financial gain, political reasons)
- nation state – steal sensitive information to influence populations and damage critical infrastructure for political gain
- hacktivists – expose or draw awareness to government agencies or businesses and are motivated by using their findings 'for good'
- script kiddies – novices who are experimenting in the field will conduct attacks for the challenge and thrill of breaking into networks illegally

- the importance of threat intelligence – the process of gathering critical information to help analyse and prioritise potential threats:
  - enables the identification of previously unknown or emerging threats
  - provides knowledge of threat actors and their motivations
  - supports decision making to mitigate threats quickly and effectively

K2.4 The stages and application of a vulnerability assessment:

- identification of vulnerability:
  - analysis of scans and logs to check for anomalies
- analysis of vulnerability:
  - checking if the vulnerability can be exploited and assessing the severity
- identification of risks associated with vulnerabilities:
  - prioritisation of risks
- remediation:
  - updating or removing affected hardware/software
- mitigation:
  - application of appropriate countermeasures:
    - close down mitigated vulnerabilities
    - escalate vulnerabilities that still pose a threat

K2.5 The application of the Common Vulnerabilities and Exposures (CVE) technique to evaluate the results of a vulnerability assessment:

- identification of known CVEs published (for example, published by vendor, penetration tester)
- research into CVE:

Knowledge – What you need to teach

- performance of a risk assessment based upon the Common Vulnerability Scoring System (CVSS) scores – a score which ranks vulnerabilities on a scale of 0 to 10.0 depending on their impact, ease of exploitation and severity
- identification of systems affected
- identification of mitigations

- implementation of suggested mitigations

K2.6 Factors to consider when making recommendations for mitigations based upon the evidence provided by vulnerability assessment tools:

- potential risks and impact on business, operations and infrastructure
- mitigating circumstances leading to the vulnerability
- cost of implementing or not implementing the recommendations
- type and severity of the vulnerability
- availability of resources:
  - people
  - finances
  - technology
- timeframes – obligations for reporting and response time based upon findings
- the scope and priority based upon the CVE score
- potential mitigation responses
- results from a proof-of-concept (PoC) simulation – completed to confirm flaws in a network

K2.7 The potential impacts that an exploited vulnerability might have on an organisation:

- damage to property and resources – damage to property, infrastructure and resources caused by safety risks or vulnerabilities within control systems
- financial loss – loss of income due to inability to continue or perform normal business functions
- reputational damage – harm to an organisation's public image and loss of customer trust following exposure of sensitive or personal information
- fines or prosecution – fines by a court or regulating body due to non-compliance (for example, a fine from the Information Commissioner’s Office (ICO) because of a data breach)
- operational disruption – an organisation's inability to conduct its day-to-day operations and perform normal business functions
- harm to employees:

Knowledge – What you need to teach

- physical harm – harm caused to an individual due to vulnerabilities in control systems (for example, interference with fire defence systems)
- psychological harm – exposure of an individual's sensitive data resulting in psychological harm

- identity theft – an employee's personal information being stolen because of a vulnerability (for example, taking out loans or credit cards in their name)

K2.8 The purpose of vulnerability assessments on network infrastructure:

- host based – identifies vulnerabilities in workstations, servers or other network hosts and provides visibility into configuration settings and patch history
- network based – identifies potential network security attacks and vulnerable systems on networks
- wireless based – identifies rogue access points and confirms that a company's network is securely configured
- application based – identifies known software vulnerabilities and misconfigurations in network or web apps (for example, structured query language (SQL) injection)

K2.9 The strengths and weaknesses of vulnerability assessment tools:

- infrastructure scanners – applied to host, network and wireless infrastructure:
  - strengths:
    - identifies missing patches
    - identifies unsupported systems
    - discovers weak passwords
    - provides exposure of services
    - discovers missing hardening measures
    - identifies incorrect access controls
  - weaknesses:
    - does not protect against malicious attacks
    - only discovers threats that have previously been identified
    - vendor fixes can take a long time to implement
    - potential for inaccuracy of results
    - potential to affect services on devices during scans
- web application scanners – applied to applications and network infrastructure:
  - strengths:
    - automatic scanning process
    - discovers SQL injection

Knowledge – What you need to teach

        - identifies if authentication is not functioning correctly
        - highlights exposure of data
        - identifies incorrect access controls
        - discovers vulnerable third-party use
        - identifies weak or unencrypted communications
    - weaknesses:
        - identifies a vulnerability when one is absent (for example, false positives)
        - fails to identify a vulnerability when one is present (for example, false negatives)
        - impacts on system resources during scanning process
        - only discovers threats that have previously been identified
- software scanners – applied to applications:
    - strengths:
        - discovers missing updates
        - identifies missing patches
        - performs vendor specific checks
    - weaknesses:
        - regular updates are required
        - identifies a vulnerability when one is absent (for example, false positives)
        - fails to identify a vulnerability when one is present (for example, false negatives)
        - difficult to identify the impact the vulnerability will have on the business and infrastructure

K2.10 Types of potential risks within an organisation and the associated management approaches:

- compliance risks – not implementing or adhering to policies and procedures:
    - monitoring and updating of processes and procedures
    - controls to monitor compliance
    - exception reports – a report that highlights to management the potential upcoming issues before they become major problems (for example, software support about to expire)
- safety risks – harm to individuals, property or the environment:
    - consistent checks for human error
    - auditing of maintenance processes
- information security risks – an incident/event that results in business information being lost, stolen, copied or otherwise compromised:

Knowledge – What you need to teach

- control measures for data (for example, access controls)
- monitoring of network traffic
- device management (for example, restricted USB access)
- regular and effective information security training

K2.11 Potential threats and mitigation approaches to prevent privacy breaches:

- social engineering:
  - raising awareness of recent cyber issues
- unmanaged devices:
  - introduction of company policies to ensure unmanaged devices aren't used
  - providing staff with secure devices
- untrained staff:
  - undertaking training of staff
  - production of SOPs
- insider threats:
  - implementing appropriate access controls
  - monitoring unusual activity
  - segregation of duties
- insecure unpatched applications:
  - ensuring all patches and updates are installed
- third-party risk (for example, a cloud organisation handling data):
  - undertaking due diligence checks of suppliers prior to use
- improper disposal of devices:
  - securely wipe devices prior to disposal
  - adhering to relevant legislation (for example, Data Protection Act 2018)

K2.12 The purpose of measures used in risk management to assess the impact of threats and vulnerabilities:

- recovery time objective (RTO) – a way of measuring how much time it takes after the disaster has occurred to recover systems to an acceptable operational state
- recovery point objective (RPO) – a way of measuring loss tolerance and how much data can be lost or manually recovered

Knowledge – What you need to teach

- mean time between failures (MTBF) – a way of anticipating the likelihood of an asset failing or how often a failure may occur
- mean time to detect (MTTD) – a way of measuring how efficient the detection capabilities are
- mean time to recovery (MTTR) – a way of measuring the average time it takes to maintain and restore a failed system

K2.13 The factors to consider in the identification and classification of critical systems:

- single point of failure within an organisation's system – the potential risks posed by a flaw in the design, implementation or configuration of a system, where a single point is depended upon
- mission essential functions of an organisation – functions that must be continued throughout or resumed rapidly, after a disruption to normal operations

K2.14 Potential factors involved in threat assessment to support information security:

- environmental:
  - power failure
  - power spikes
  - natural disasters
  - fire
  - equipment failure
  - flooding
- manmade:
  - internal:
    - malicious or inadvertent activity from employees
    - human error
    - misconfigured firewall settings
  - external:
    - malware
    - attack
    - social engineering
    - terrorism

K2.15 The application of qualitative and quantitative approaches and tools for the analysis of threats and vulnerabilities:

- approaches:
  - qualitative – applied to business risks through non-numeric methods:

Knowledge – What you need to teach

- determination of severity of threats and vulnerabilities using RAG rating:
  - red – high risk requiring immediate action
  - amber – moderate risk that needs to be observed closely
  - green – low risk with no immediate action required
- quantitative – applied to business risks through numerical methods:
- determination of the effects of threats and vulnerabilities using numerical methods (for example, cost overrun, resource consumption):
  - calculation based on single loss expectancy (SLE) x annual rate of occurrence (ARO) = annual loss expectancy (ALE)
  - use of CVSS – a score which ranks vulnerabilities on a scale of 0 to 10.0 depending on their impact

- tools:
  - fault tree analysis – a graphical representation used to analyse the causes of a system level failure
  - failure mode, effects and criticality analysis (FMECA) – a structured method used to assess the causes of failures for a product or process and the effect on production, safety, cost and quality
  - CCTA Risk Analysis and Management Method (CRAMM) – a risk analysis methodology that comprises 3 stages; the first 2 scope and evaluate the risk and the third recommends counter measures
  - Factor Analysis of Information Risk (FAIR) – a model for understanding, analysing and quantifying cyber risk and operational risk in qualitative terms

K2.16 The process and application of a security risk assessment:

- process:
  - identification of potential security risks that might occur
  - assessment of the security risks using a scoring matrix:
    - likelihood – probability of a security risk happening
    - severity– impact of an incident/event on the organisation
    - calculation of the overall risk rating:
      - likelihood x severity = risk score/RAG rating
  - assessment of the asset value versus the potential mitigation controls
  - control of the security risks – responses must be proportionate to risk and value
  - record of the findings

Knowledge – What you need to teach

- regular review and test of the controls

- application – performing regular security risk assessments using internal or external auditors to cover key business areas (for example, in-house computer systems and third-party suppliers)

K2.17 The stages and application of penetration testing in vulnerability assessments:

- planning and scoping – identification of rules of engagement, timings, legalities and contractual obligations
- reconnaissance – investigation of business and operations with the purpose of gathering information about the system (for example, network topology, operating systems, applications)
- scanning – utilisation of various tools to identify open ports and network services on the system
- vulnerability assessment – scanning of the system to identify potential vulnerabilities and determine whether they can be exploited to gain access
- exploitation – attempts are made to exploit the vulnerability and access the system
- reporting – creation of documentation that details the findings of the penetration test and provides recommendations to fix or mitigate any vulnerabilities found in the system

K2.18 The types of risk response utilised within cyber security:

- accept – the impact of the risk is deemed acceptable when there is no mitigation available, or the relevant mitigation has been applied and there is still a risk remaining
- transfer – the outsourcing of the risk to another party to manage, lower or offset the risk
- avoid – changing the scope of a project or system to avoid the identified risk
- mitigate – reducing the severity or likelihood of the identified risk by implementing relevant controls or measures

K2.19 The stages and process of incident/event management:

- identification of the incident/event (for example, via service desk, phone calls, emails, SMS, live chat messages)
- logging of the incident/event:
  - manual (for example, raising a ticket):
    - contact details of the individual raising the ticket
    - date and time of the incident/event
    - description of the incident/event
  - automatic (for example, raised by a monitoring system):
    - date and time of the incident/event
    - description of the incident/event

Knowledge – What you need to teach

- management of the incident/event:
  - creation of incident/event ticket and allocation of ticket number, to allow for tracking
  - assignment to relevant personnel (for example, technician):
    - based on relevant expertise, level of system access and seniority of personnel
    - breakdown of task as required (for example, into sub-activities)
  - categorisation of the incident/event:
    - based upon the disruption that may be caused to the business or a service (for example, disruption to one business area or one area of the network, or disruption to all business areas and all areas of the network)
- prioritisation of the incident/event:
  - high risk requiring immediate action
  - moderate risk that needs to be observed closely
  - low risk with no immediate action required
  - service level agreement (SLA) management and escalation:
    - conformance and compliance with SLA of task
    - variance against SLA escalated to appropriate personnel
  - escalation:
    - determine if the incident/event needs to be escalated within or outside of the IT team
    - escalate the incident/event to the relevant authorities as appropriate:
      - crimes – reported to the police
      - data breaches – reported to the ICO
- resolution of the incident/event:
  - temporary workaround or permanent solution
- closure of the incident/event:
  - confirmation of incident/event resolution
  - confirmation from user, if applicable
  - population of incident/event report, summarising:
    - executive summary:
      - a high-level overview to management summarising the report content without too many technical details
    - discovery:

Knowledge – What you need to teach

- discovery of the incident/event
- the investigation that has been undertaken

▪ impact:

- the affect the incident/event has had on the business

▪ mitigation:

- the actions that have been taken

▪ recommendations:

- the suggested measures to reduce the chances of a repeat incident/event

▪ ongoing risks:

- details of any outstanding risks

K2.20 The application of the NCSC Cyber Essentials controls:

- boundary firewalls and internet gateways – applied to restrict the flow of traffic in systems
- secure configuration – applied to ensure users have only the required functionality (for example, removing unnecessary software, configuration to limit web access)
- malware protection – applied to maintain up-to-date anti-malware software and regular scanning
- security update management – applied to maintain system and software updates to current levels
- access control and management – applied when restricting access to a minimum, based on user attributes (for example, principle of least privilege, username and password management) – when special access is required above the standard user, then Privileged Access Management (PAM) would be implemented (for example, super user account, privileged business user)

K2.21 The types and application of encryption tools as a risk mitigation technique:

- asymmetric encryption – applied to send private data from one user to another (for example, encrypted email systems):
  - data in transit encryption:
    - transport layer security (TLS) – applied to encrypt end-to-end communication in email, websites and instant messaging
    - secure sockets layer (SSL) – a legacy protocol applied to create an encrypted link between a website and a browser using security keys for businesses to protect data on their websites
- symmetric encryption – applied to encrypt and decrypt a message using the same key (for example, card payment systems):
  - data at rest encryption (DARE):

Knowledge – What you need to teach

- full disk encryption (FDE) – applied to encrypt the entire contents of a computer, used in situations to ensure that no data can be left unencrypted on a device (for example, this mitigates against theft of a laptop computer)
- file based encryption (FBE) – applied to encrypt individual files and folders, can be used when transferring sensitive documents between computers and individuals to prevent eavesdropping or tampering

K2.22 The purpose, criteria and types of back-ups utilised in risk mitigation:

- purpose:
  - to maintain an up-to-date copy of data to enable future recovery and restoration for full disaster recovery or partial data loss
- criteria:
  - frequency – a schedule signalling the required periodic back-up (for example, daily, weekly, monthly)
  - source – the information that is being backed up (for example, files or data)
  - destination – the internal or external location of the information
  - storage – the information must be stored safely in an appropriate format (for example, magnetic tape, disk) and location (for example, onsite, cloud, secondary site) ready for restoration as required
  - retention – the length of time the backed-up data is retained
  - test – the testing of restores on a regular basis to ensure that a back-up will be ready in the event of a disaster
- types:
  - full – the creation of at least one additional copy of information
  - incremental – a back-up of only the information that has changed since the previous full or incremental backup
  - differential – a back-up of files that have changed since the last full backup
  - mirror – a back-up of the information at a given time
  - immutable – a back-up that cannot be changed, overwritten or deleted

K2.23 The purpose of organisational digital use policies and procedures to support risk mitigation:

- data protection policy – standardises the use, monitoring and management of data
- acceptable use policy – provides information on the way in which networks or infrastructure should be used
- access control policy – provides information on how access and permissions of users is managed

Knowledge – What you need to teach

- asset classification policy – influences the amount and complexity of controls that are applied to protect the asset, access controls, disposal and recovery objectives
- information security policy – outlines requirements to use networks and infrastructure in a secure way
- incident response procedure – outlines how an organisation will respond to an incident/event
- mobile device policy – details standards, procedures and restrictions for users connecting mobile devices to organisational infrastructure
- back-up policy – details standards and procedures for performing backups to prevent loss of data
- bring your own device (BYOD) policy – details requirements and restrictions when undertaking work activities using personally owned devices
- password policy – provides information on computer security by requiring users to utilise strong passwords
- asset disposal policy – provides guidance on the secure disposal of hardware when no longer in use
- data retention policy – determines how long certain types of data must be kept

Skills – What you need to teach

The student must be able to:

S2.1 Identify and categorise threats, vulnerabilities and risks:

- identify potential threats, vulnerabilities and risks
- calculate the likelihood and severity of the identified threats, vulnerabilities and risks
- analyse and categorise the priority based on level of risk

(GMC1, GMC2, GMC3, GMC6, GMC8, GDC4)

S2.2 Escalate information about security incidents/events whilst preserving evidence:

- record details of incident/event:
  - the date and time of the incident/event
  - a description of the incident/event
- take appropriate action:
  - isolate the device from the network if required
- preserve the digital evidence:
  - take a copy of relevant digital log files

Skills – What you need to teach

- escalate the incident/event as appropriate

(GMC5, GDC1, GDC5)

S2.3 Scope, document and evaluate results of vulnerability assessments:

- identify the scope of vulnerability assessment information:
  - identify the systems, services and networks that are in scope for the assessment
  - identify access requirements
  - identify the vulnerabilities that the systems will be tested against
- evaluate the results of the vulnerability assessment information:
  - classify the risks posed by any identified vulnerabilities
  - determine the business impact the vulnerability could have on an organisation (for example, loss of data)
- document and organise results of the vulnerability assessment

(GEC3, GEC4, GMC5, GDC4)

S2.4 Provide recommendations based upon the evidence provided by vulnerability assessment tools:

- considering:
  - risks and impacts
  - mitigating circumstances
  - cost of implementing the recommendations
  - type and severity of vulnerability
  - the availability of resources
  - timeframes
  - scope and priority based on CVE score
  - potential mitigation responses
  - results from the proof-of-concept simulation
- document recommendations logically and coherently, and communicate using appropriate terminology to required audiences

(GEC1, GEC2, GEC4, GEC6, GMC10, GDC3, GDC6)

S2.5 Document incident/event and exception information in appropriate format:

- gather information relevant to incident/event or exception
- complete management reports in line with organisational policies and procedures:
  - incident/event report

Skills – What you need to teach
○ exception report • store in line with data protection **S2.6 Utilise a compliance and monitoring plan to monitor cyber security compliance:** • audit processes and policies to ensure they remain up to date (for example, review of information security policy): ○ improve and maintain processes and policies as required • compare and check accuracy of processes, log files and incident/event reports • comply with ISO standards

Performance outcome 3: Discover, evaluate and apply reliable sources of knowledge

Knowledge – What you need to teach
The student must understand: **K3.1 A range of potential sources of knowledge applicable to cyber security:** • academic publications (for example, textbooks, research journals and periodicals) • supplier literature (for example, Microsoft, Amazon Web Services) • websites (for example, wikis, forums, community encyclopaedias, manufacturers' websites, question and answer websites) • webinars (for example, information sharing by industry professionals) • social media (for example, company profiles for Twitter, Facebook and LinkedIn) • blogs (for example, discussions around vulnerabilities) • vlogs (for example, tutorials on cyber security mitigation strategies) • professional networks (for example, cyber security networking events/conferences) • professional bodies (for example, Chartered Institute of Information Security (CIISec), CREST, ISACA, UK Cyber Security Council) • e-learning (for example, massive open online courses (MOOCs)) • peers (for example, colleagues, network contacts, other industry professionals) • cyber security policies and procedures (for example, information security policy) • guidelines and legislation (for example, Data Protection Act 2018)

Knowledge – What you need to teach

- regulating authorities (for example, ICO)
- industry standards (for example, NCSC Cyber Essentials, CIS Benchmarks)
- industry accreditation (for example, CompTIA, Certified Cyber Professional (CCP), (ISC)²)
- databases (for example, CVE)

K3.2 The factors of reliability and validity to be applied to legitimise the use of sources of knowledge and information:

- credibility of publisher (for example, author, organisation):
  - affiliated to specific bodies (for example, government, industry regulators)
  - reputation
  - experience (for example, relevant qualification in subject)
  - industry-certified accreditation
- supported by credible citations
- knowledge and information are relevant to the context
- currency of the publication:
  - version number (for example, use of the current version)
  - date of publication (for example, is the content outdated?)
- absence of bias – personal opinions have not influenced source or information

K3.3 The factors affecting bias:

- author/propriety bias – unweighted opinions of the author or owner
- confirmation bias – an individual may search for, interpret, favour and recall information that reinforces or confirms their prior beliefs or values
- selection bias – refers to the inclination to select individuals, groups or data in a way that randomisation is not achieved
- cultural bias – implicit assumptions based on societal norms
- availability bias – an individual's opinion based on most recent or vivid experiences or memories

K3.4 The application of potential evaluation techniques and tools:

- evaluation techniques:
  - triangulation – validation of data or information by cross-checking from more than 2 sources to check the consistency of the results from different sources
  - formative evaluation – an evaluation that takes place before or during the implementation of a task to make improvements

Knowledge – What you need to teach

- summative evaluation – an evaluation that takes place at the end of a task to review achievements and inform future actions
- observation – reviewing and monitoring of a task in real time
- corroboration – the strengthening of existing information by cross-referencing information from other sources
- conclusions – a summary of the accuracy or appropriateness of the results
- recommendations – suggestions for future actions and decisions (for example, information security training)

- evaluation tools:
  - gap analysis – to assess the current situation of existing control measures compared to a desired situation
  - maturity assessments – to measure an organisation's ability to meet predictable outcomes
  - user diaries – to provide a timely and accurate documentation of an ongoing process

K3.5 The key stages of critical thinking to support objective evaluation:

- identification of relevant information:
  - different arguments, views and opinions
- analysis of identified information:
  - considering bias and objectivity
  - establishing links between information and data
- selection of relevant evaluation techniques and tools
- evaluation of findings
- drawing conclusions

K3.6 Types and purpose of potential communication methods used to share cyber security information and knowledge:

- digital services – digitally based technology that supports communication and enables 2-way communication:
  - helpdesk
  - phone
  - emails
  - SMS
  - chat messages

Knowledge – What you need to teach

- social media channels – supports conversations, community, connecting with an audience and building relationships:
  - organisational
  - public
  - community
  - personal
- knowledge bases and knowledge management systems – a repository of information produced by one or more authors:
  - wikis
  - cyber security body of knowledge (CyBOK)
  - MITRE ATT&CK
  - blogs
  - information security training platform
  - industry/vendor subscriptions or updates
- project management tools – to communicate, track and visualise key information and progress throughout a task or project:
  - issue logs
  - Gantt charts
  - Kanban boards
  - burndown charts

K3.7 The potential impacts of cyber security issues on critical national infrastructure:

- supply chain:
  - disruption to the supply of food and raw materials
- utilities:
  - energy sources:
    - power cuts
    - surges
    - under-voltage events
    - restricted or loss of gas supply
  - water and sanitation:
    - loss of fresh water to homes

Knowledge – What you need to teach

        - flooding
        - disruption to water treatment/facilities
    - government:
        - interruptions to national communication channels
        - interruptions to implementation of policies
    - finance:
        - failure of scheduled payments
        - interruption to electronic transfers
        - inability to process physical payments
    - healthcare:
        - compromised confidentiality, loss or damage to patient records
        - impact on communications and ability to treat patients
    - communication technologies and internet service providers:
        - loss of service
        - interruptions to businesses and individuals
        - eavesdropping
        - impersonation
    - defence:
        - impact on country's military and defence capabilities
    - transport:
        - disruption to privately or publicly owned modes of transport (for example, buses, trains, airlines)
    - emergency services dispatch:
        - disruption to response times and capabilities

K3.8 The purpose and types of control systems:

- purpose:
    - to receive data from remote sensors
    - to measure values
    - to control a process or an asset, where required, across different locations
- types:
    - industrial control systems – supports critical national infrastructure

Knowledge – What you need to teach

- medical control systems – supports control of life sustaining equipment and patient data
- facility related control systems – supports control of securing facilities (for example, door locks)
- automotive control systems – controls everything in a vehicle (for example, engine and fuel systems)

K3.9 Evolving cyber security risks associated with internet of things (IoT) devices:

- poor data protection controls:
  - devices often have insufficient security controls built in to protect them from threats
  - devices are usually too low-powered to support encryption and often give access to shared networks
- poor password protection:
  - weak or predictable passwords (for example, use of factory setting password)
- insecure data transfer and storage:
  - during processing, transit, or at rest, sensitive data is not encrypted or controlled by the system
- security updates:
  - lack of ability to securely update the device; as a result, firmware is not validated on devices, secure delivery is not secured, anti-rollback mechanisms are not in place and security updates are not notified of security changes

K3.10 The importance of information assurance and governance (IAG):

- guides the development and improvement of IAG strategies, policies and processes
- supports the auditing of current IAG strategies, policies and processes
- informs the maintenance of IAG strategies, policies and processes through compliance monitoring plan
- provides confirmation of compliance (for example, with ISO standards, NIST cyber framework)

Skills – What you need to teach

The student must be able to:

S3.1 Identify 3 sources of knowledge:

- identify the purpose and parameters of the topic or scenario
- identify 3 appropriate sources of knowledge to support the topic or scenario (for example, websites, community encyclopaedias, question and answer websites)

Skills – What you need to teach

(GMC5, GDC3, GDC5)

S3.2 Compare sources and recommend actions to ensure reliability and validity of sources:

- compare sources by applying the factors of reliability and validity:
  - credibility of publisher (for example, author, organisation)
  - currency of publication
- recommend and justify actions to ensure the most reliable and valid source is utilised (for example, which sources may or may not be valid and reliable and why, whether there is a requirement to find additional sources)

(GMC5, GMC6, GDC5)

S3.3 Search for information from sources to support a topic or scenario:

- identify requirements of topic or scenario
- search sources and extract relevant information (for example, information on threat intelligence, common attack techniques, cyber security policies and procedures, relevant guidelines, legislation and standards, evolving cyber security issues)

(GMC5, GDC1, GDC6)

S3.4 Analyse information from sources of knowledge and recommend actions to ensure reliability and validity of information:

- analyse information from sources of knowledge and apply the factors of reliability and validity to the information:
  - supported by credible citations
  - the absence of any bias within the information:
    - author/propriety bias
    - confirmation bias
    - selection bias
    - cultural bias
    - availability bias
- recommend and justify actions to ensure the most reliable and valid information is utilised (for example, which information may or may not be valid and reliable and why, whether there is a requirement to find additional information)

(GMC6, GDC5)

S3.5 Corroborate information across multiple sources:

- cross reference the identified information across multiple sources to identify:

Skills – What you need to teach
○ similarities and differences of key information (GMC3, GMC5, GMC6, GDC3, GDC5) **S3.6 Demonstrate critical thinking within a cyber security context:** • identify relevant information • analyse relevant information • select and use evaluation techniques and tools • evaluate and summarise findings • logically organise and record conclusions (GEC1, GEC3, GEC4, GEC6, GMC1, GMC2, GMC3, GMC8, GMC10, GDC4)

Section 5: TQ glossary

TQ specification

Route core

The core knowledge and understanding across the technical qualification route.

Pathway core

The core knowledge and understanding across the technical qualification pathway.

Occupational specialism core

The requirements for the technical qualification occupational specialism.

Student

The person studying the technical qualification (‘The student must…’).

Tutor

The individual delivering the technical qualification.

Provider

The centre delivering the technical qualification.

Series

Assessments which must be attempted in the same assessment window, for example paper A and paper B of the core examination.

Assessment mode

The assessment mode is how an assessment is made available and/or administered to students. For example a written examination can be administered to students via an on-screen platform or via a traditional paper-based document.

Section 6: Additional information

Annual monitoring visits

Our quality assurance team will monitor all approved TQ providers on an ongoing basis. All providers delivering the TQ will be quality assured at least once a year to ensure that they are delivering in line with required standards. Annual monitoring reviews will be carried out either face-to-face or remotely by quality assurers appointed, trained and monitored by us. Providers will be allocated a quality assurer upon approval. Our quality assurers will complete a report following each annual review to record and share their findings.

Guided learning hours (GLH)

Guided learning is the activity of a student being taught or instructed by – or otherwise participating in education or training under the immediate guidance or supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training.

For these purposes, the activity of 'participating in education or training' shall be treated as including the activity of being assessed, if the assessment takes place under the immediate guidance or supervision of a lecturer, supervisor, tutor or other appropriate provider of education or training.

Total qualification time (TQT)

Total qualification time is an estimate of the minimum number of hours that an average student would require in order to complete a qualification.

TQT comprises:

- the GLH for the qualification
- an estimate of the number of hours a student will likely spend in preparation, study or any other form of participation in education or training, including assessment, which takes place as directed by – but not under the immediate guidance or supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training

Essential skills

While completing this qualification, students may develop the knowledge, understanding and essential skills employers look for in employees. These range from familiar 'key skills', such as team working, independent learning and problem solving, to more tricky-to-measure skills, such as:

- appropriate workplace behaviour and dress
- appropriate interpersonal skills
- communicating with professional colleagues/peers and/or hierarchical seniors
- supporting other aspiring employees

- personal manners
- understanding work practices and how different roles and departments function within an organisation

Recognition of prior learning (RPL)

Recognition of prior learning (RPL) may be applied to the core content only.

Providers may, at their discretion, recognise prior learning if they are satisfied that the evidence provided meets the qualification's requirements.

For more information, please refer to the recognition of prior learning (RPL) credit accumulation and transfer (CAT) policy on the Policies & Documents page on the NCFE website.

Qualification dates

We review qualifications regularly, working with sector representatives, vocational experts and stakeholders to make any changes necessary to meet sector needs and to reflect recent developments.

If a decision is made to withdraw a qualification, we will set an operational end date and provide reasonable notice to our providers. We will also take all reasonable steps to protect students' interests.

An operational end date will only show on the regulator's qualification database and on our website if a decision has been made to withdraw a qualification. After this date, we can no longer accept student registrations.

This qualification has external assessments, which can only be taken up to the last assessment date set by us. No external assessments must be permitted after this date, so students must be entered in sufficient time. Please visit the NCFE website for more information.

Staffing requirements

Providers delivering any of our qualifications must:

- have a sufficient number of appropriately qualified/experienced tutors to deliver the TQ to the volume of students they intend to register
- have experience of delivering level 3 qualifications and preparing students for written and project-based assessments
- ensure that all staff involved in delivery are provided with appropriate training and undertake meaningful and relevant continuing professional development
- implement effective processes to ensure all delivery is sufficient and current. This should include standardisation to ensure consistency of delivery
- provide all staff involved in the delivery process with sufficient time and resources to carry out their roles effectively
- ensure staff have an industry focus when delivering content

Core staffing requirements

Staff involved in the delivery of the core content must be able to demonstrate that they have (or are working towards) the relevant occupational knowledge and/or occupational competence in digital support services at the same level of higher than the qualification being delivered. This may be gained through experience and/or qualifications. Understanding of the wider digital sector would be beneficial, including:

- relevant legislation
- emerging technologies within the digital sector
- industry standard operating procedures
- cloud technologies
- application of digital approaches and solutions to problem solving
- network principles and architecture
- data analytics and how data driven decisions influence business decision making
- project management (specifically within the digital sector)

Occupational specialism staffing requirements

Staff involved in the delivery of the occupational specialism content must be able to demonstrate that they have (or are working towards) the relevant occupational knowledge and/or occupational competence in the relevant occupational specialism area at the same level or higher than the qualification being delivered. This may be gained through experience and/or qualifications, including:

- copper and fibre optic cabling installation, testing and tools
- EIA/TIA standards
- network principles and architecture
- cyber security principles and standards

Resource requirements

Providers must ensure that the student has access to the necessary materials, resources and workspaces for delivery and assessment of mandatory knowledge and skills. The following lists are not exhaustive. Please refer to the qualification content for a more detailed indication of the required resources.

General:

- computer with appropriate access rights
- internet access
- audio/visual recording equipment

Core:

- software:
  - word processing (for example MS Word, Google Docs)
  - presentation (for example MS PowerPoint, Google Slides)
  - spreadsheet (for example MS Excel, Google Sheets)
  - project management (for example MS Excel, MS Project)
  - basic image editing software (for example Adobe Photoshop, GIMP)
  - programming software
  - database software (for example MS SQL, MySQL)
  - web browsers
- access to a range of data sources (for example online, social media, analytical)
- internet access
- access to a range of research resources (for example online, books, journals)
- access to hardware with appropriate specifications (for example PC, laptops, mobile devices)
- access to a web server
- personal protective equipment (PPE)

Occupational specialism – Digital Infrastructure:

- software:
  - appropriate network management software (for example load balancing software)
  - network diagramming software (for example Visio, Packet Tracer)
  - operating systems
  - vulnerability scanning software
  - anti-malware software
  - firewall software
  - remote access software
  - intrusion detection software
  - desktop virtualisation software
  - virtual machines
- hardware:

- access to appropriate network architecture devices (for example server, switch, hub, firewalls, load balancer, WAP)
- access to a range of copper cables
- access to a range of connectors
- access to WiFi connectable devices
- media to support installation and deployment of operating systems
- computers capable of running virtual machines via a hypervisor

- tools:
  - cabling terminating tools (for example wire cutters, crimping tools)
    - cable testing tools (for example network cable tester, tone generator and probe)
- PPE

Occupational specialism – Network Cabling:

- software:
  - Packet Tracer
  - firewall software
  - testing software
- hardware:
  - access to appropriate network architecture devices (for example server, switch, hub, firewalls, load balancer, WAP)
  - access to copper and fibre-optic cable
  - access to digital cameras
  - access to a range of cable connectors
  - patch panel
- tools:
  - cabling terminating tools (for example wire cutters, crimping tools)
  - cable testing tools (for example network cable tester, tone generator and probe)
  - optical loss test set (tier 1)
  - optical time domain reflectometer (tier 2)
  - fibre inspection tool
  - access to telecommunications fixtures and fittings (for example cabinets, trunking)
  - label making machine for labelling cables

- access to physical access equipment:
  - low level access towers
  - mobile elevating work platforms (MEWPs)
- PPE

Occupational specialism – Digital Support:

- software:
  - appropriate network management software (for example Packet Tracer, load balancing software)
  - operating systems
  - vulnerability scanning software
  - anti-malware software
  - firewall software
  - remote access software
  - intrusion detection software
  - email software
  - instant messaging software
  - screen capturing recording software/equipment
  - collaboration software
- hardware:
  - mobile devices
  - media to support installation and deployment of operating systems
  - access to appropriate network architecture devices (for example server, switch, hub, firewalls, load balancer)
  - digital camera
  - USB storage devices with minimum of 16GB
- PPE

Occupational specialism – Cyber Security:

- operating systems
- software for end user devices and servers
- anti-virus software
- anti-malware software

- vulnerability scanning software
- firewall software
- network diagramming software (packet tracer)
- access to data sources
- access to physical or virtual server
- access to computers capable of virtualisation
- desktop virtualisation software
- USB drives/pens
- access to WiFi

Customer support team

Our customer support team will support you with approvals, registrations, moderation, external assessment, results and general queries.

Fees and pricing

Fees will be made available to eligible and approved providers.

Training and support for providers

Our provider development team's primary purpose is to support providers and teaching teams in the delivery of this qualification. There are a number of ways in which we can do this, which include:

- providing bespoke one-to-one support with the delivery staff
- delivering face-to-face events at numerous locations throughout the country
- facilitating delivery and CPD webinars
- signposting you to teaching and learning resources
- providing you with delivery updates on the technical qualification

The variety of support available includes:

- content structure
- teaching strategies
- SEN guidance
- quality assurance
- assessment preparation and blended learning

Should you wish to discuss your teaching and delivery requirements, please email: provider.development@ncfe.org.uk.

Useful websites and sources of information

Information Commissioner's Office (ICO): https://ico.org.uk/

IEEE: http://www.ieee.org/

Telecommunications Industry Association (TIA): https://tiaonline.org/

Scrum: http://www.scrum.org/

Google Quantum AI: https://quantumai.google/

The National Cyber Security Centre: http://www.ncsc.gov.uk/

Digital, Data and Technology Profession Capability Framework: www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework

Cisco: www.cisco.com/c/en_uk/index.html

DataViz: https://datavizproject.com/

Learning resources

We offer a wide range of bespoke learning resources and materials to support the delivery of this qualification, which include:

- schemes of work
- tutor delivery guides

For more information on the resources being developed for this qualification, please check the qualifications page on the NCFE website.

Equal opportunities

We fully support the principle of equal opportunities and oppose all unlawful or unfair discrimination on the grounds of ability, age, colour, culture, disability, domestic circumstances, employment status, gender, marital status, nationality, political orientation, racial origin, religious beliefs, sexual orientation and social background. We aim to ensure that equality of opportunity is promoted and that unlawful or unfair discrimination, whether direct or indirect, is eliminated both in our employment practices and in access to qualifications. A copy of our diversity and equality policy is available on request.

Diversity, access and inclusion

Our qualifications and associated assessments are designed to be accessible, inclusive and non-discriminatory. We regularly evaluate and monitor the 6 diversity strands (gender, age, race, disability, religion, sexual orientation) throughout the development process as well as throughout the delivery, external quality assurance and external assessment processes of live qualifications. This ensures that positive attitudes and good relations are promoted, discriminatory language is not used and our assessment procedures are fully inclusive.

Reasonable adjustments and special considerations policy

This policy is aimed at anyone who uses our products and services and who submits requests for reasonable adjustments and special considerations. Students who require reasonable adjustments or special consideration should discuss their requirements with their tutor.

The most up-to-date version of the policy can be found on the NCFE website where providers can find details of how to request a reasonable adjustment or special consideration.

Contact us

NCFE

Q6

Quorum Park

Benton Lane

Newcastle upon Tyne

NE12 8BT

Tel: 0191 239 8000*

Fax: 0191 239 8001

Email: tlevelsupport@ncfe.org.uk

Websites: www.ncfe.org.uk

Version 2.0 19 June 2023

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

Owner: Qualification Development Manager

Change history record

Version	Description of change	Approval	Date of issue
v1.0	Post approval, updated for publication		December 2020
v1.1	Update of section: About this TQ Specification to remove draft information		January 2021
v1.2	Updates to Sections 1 and 4 (Institute reference: ODSR_DSS_002-ODSR_DSS_005)		March 2021
v1.3	Branding updated Updates to Sections 1, 2, 4, 5 and 6 (Institute reference ODSR_DSS_007-ODSR_DSS_034)		September 2021
v1.4	Updates to language relating to GLH in section 2. Updates to resources list in section 6. (Institute reference ODSR_DSS_036-039, ODSR_DSS_036-042-43)	October 2021	January 2022
v1.5	Assessment requirement clarification (ODSR_DSS_117)	December 2021	March 2022
v2.0	The following amendments have been made to this qualification specification following annual review. **General changes:**	May 2023	19 June 2023

	• the Cyber Security occupational specialism has been added to this qualification specification • clarification provided regarding registering students on T Levels and transferring between T Levels and occupational specialisms • updates have been made to grading tables and grade descriptors • legislation or regulations have been updated with current dates, where applicable • updated websites and sources of information • updated resource requirements • updated training and support for providers information • updated assessment information **Amendments made to the core component section:** • in R1.10, reference to 'user experience' has been updated to 'improved user experience' • in R5.1, reference to 'redundant array of independent disks (RAID) card' has been removed • in R5.3, 'User Datagram Protocol (UDP)' has been included • in R7.2, reference to 'green computing' has been added • in R10.3, reference to 'social engineering' has been added • in R12.1, reference to 'sprints' has been removed **Amendments made to the Digital Infrastructure occupational specialism section, including:** • in K1.7, updates have been made to provide further clarification about the phases of penetration testing • in K1.13, reference 'risk matrix - used to calculate the RAG rating for a risk' has been added • in K2.2, additions have been made to wireless bands and channels		

	• in K2.3, reference to 'removable media' has been removed **Amendments made to the Network Cabling occupational specialism section, including:** • in K1.16, updates have been made to provide further clarification about the phases of penetration testing • in K2.10, reference to 'cheaper material costs' has been updated to 'materials more expensive but cheaper to maintain long term' • in K2.17, reference to 'log files' has been added **Amendments made to the Digital Support occupational specialism section, including:** • in K2.10, reference to 'swap partitions' has been removed		

Schedule 3

Implementation

The content for this Schedule is contained in separate files at:

S3_GEN2W1_DSS_Implementation_Plan

S3_GEN2W1_DSS_Resource_Plan

Schedule 3

Implementation Plan

S3_GEN2W1_DSS_Implementation_Plan

Schedule 3

Resource Plan

S3_GEN2W1_DSS_Resource_Plan

Award Questionnaire Q10.7: Resource Plan - Instructions

Lot (qualification) name: Contract: T Level Technical Qualification in Digital Support Services
Potential Supplier name: Pearson Education Ltd

Introduction

The following three tabs are designed for Potential Suppliers to outline and explain their Resource Plan.

How to complete this document: Q10.7

Potential Suppliers must complete and submit one copy of this dcoument for each TQ (ie a separate response for each Lot they intend to submit a Tender for).

The three sheets that follow form the requirement of Q10.7:

>> Outline Resource Plan: Potential Suppliers are to complete all highlighted (yellow) blank boxes in the table, providing an overall outline of the proposed Resource Plan. All answers should include a level of detail that enables the Authority to assess the basis and reasonableness of the proposed strategy. For the first 6 named resources (marked as * key resources), Potential Suppliers are required to provide a named replacement resource and detail their relevant experience.

>> Blank Diagram Sheet: This sheet has been left blank for Potential Suppliers to include a diagram or picture of their resourcing and/or readiness approach should they wish to include this to further support/illustrate their Resource Plan.

>> Further 10.7 Requirements: The information requested here is designed to supplement the Resource Plan provided in Sheet 1. Potential Suppliers must complete all blank boxes, providing an appropriate amount of detail.

Schedule 4

Co-operation

1 Objective of the joint arrangements

1.1 The Supplier shall cooperate, coordinate and seek to agree certain arrangements with all third party Awarding Organisations, including the Former Supplier, involved in the delivery of the technical education qualification element of each T Level forming part of the T Levels Programme ("**T Level Awarding Organisations**") from time to time with the aim of:

1.1.1 ensuring the quality, consistency, efficiency and effectiveness of the T Levels Programme as a whole; and

1.1.2 in the interest of Students and Providers, streamlining administration relating to the T Levels Programme.

1.2 The Supplier shall ensure that all activities carried out by it under this Schedule appropriately take into account the views of each T Level Awarding Organisation (including T Level Awarding Organisations appointed subsequent and/or prior to the appointment of the Supplier) and do not risk or result in:

1.2.1 a disproportionate burden falling on any given T Level Awarding Organisation or on Providers; and/or

1.2.2 a disproportionate burden (whether by any act or omission on the part of the Supplier) on Providers and/or Students.

2 Joint arrangements

2.1 In particular, the Supplier shall (at its own cost):

2.1.1 attend a meeting convened by the Authority (on reasonable prior notice and at least once per calendar quarter) with all other T Level Awarding Organisations to discuss progress on coordination efforts including the activities set out below, and to make decisions relating to any outstanding areas of coordination;

2.1.2 in order to minimise the administrative burden on Providers, cooperate with all other T Level Awarding Organisations to coordinate and deliver an efficient method of both regular and ad hoc inspections (on an ongoing basis) of the delivery by Approved Providers of the technical education qualification element of each T Level, to ensure that the relevant Approved Providers continue to meet the requirements of their Provider Approval by the Supplier and equivalent approval by other T Level Awarding Organisations, provided always that where, as a result of such cooperation and/or coordination it is necessary for the Supplier to amend and/or modify that part of the Supplier's Response to which the provisions of paragraph 3.1.2 of Part 1 of the Service Requirements apply, then the Supplier shall obtain Approval to such amendment and/or modification;

2.1.3 coordinate and seek to agree with all other T Level Awarding Organisations (at the earliest possible date) common rules and guidance applicable to the teaching and assessment of and provision of Post-Results Services for the technical education qualification element of each T Level with the aim of having aligned rules, guidance and Post-Results Services, where appropriate, across the T Levels Programme, addressing topics such as conducting examinations;

2.1.4 share information between T Level Awarding Organisations as necessary (subject to the relevant obligations on confidentiality in this Contract) to:

(i) facilitate the joint arrangements anticipated by this Schedule;

(ii) enable transfer of achievement of the TQ Core Component of a T Level between T Level Awarding Organisations; and

(iii) enable results analysis in respect of the Route of which the TQ forms part;

2.1.5 where possible, utilise systems in the delivery of the Services which are interoperable with those utilised by other T Level Awarding Organisations so as to facilitate the portability of the Services to any Future Supplier;

2.1.6 coordinate and seek to agree with all other T Level Awarding Organisations pre-assessment access arrangements for T Levels to ensure equivalence of approach between T Level Awarding Organisations;

2.1.7 adopt a common process and, where possible, system, to that used by other T Level Awarding Organisations for applications for access arrangements for T Levels to be made and considered for the benefit of Students;

2.1.8 coordinate and seek to agree with all other T Level Awarding Organisations a common process and approach and, where possible, system to that used by other T Level Awarding Organisations, to manage and/or facilitate Reasonable Adjustments and/or applications for Special Consideration to ensure equivalence of approach between T Level Awarding Organisations;

2.1.9 seek to agree between T Level Awarding Organisations a Key Dates Schedule, such schedule to be developed in consultation with the Department, GCE Awarding Organisations, Providers and UCAS and to be Approved by the Authority;

2.1.10 attend regular meetings (at least once per calendar month unless otherwise notified by the Authority) with all other T Level Awarding Organisations to discuss operational issues in relation to the T Level Programme;

2.1.11 in order to minimise the administrative burden on Providers, co-operate with the Former Supplier, where relevant, to facilitate a smooth transition during the Entry Transition Period; and

2.1.12 where notified by the Authority, work with other T Level Awarding Organisations responsible for TQs in the same Route with the aim to, where appropriate, harmonise the common TQ Core Component across that Route.

3 Disputes relating to joint arrangements

3.1 In the event the Supplier contends that it is unable to meet its obligations under this Schedule as a result of the action or inaction of one or more third party T Level Awarding Organisation, the Supplier shall seek to resolve such matter with the relevant T Level Awarding Organisation(s). In the event that the Supplier is unable to resolve

such matter, having used its reasonable endeavours to do so, the Supplier shall promptly notify the Authority in writing with the relevant details including the steps taken to attempt to resolve the matter, and the Authority shall use its reasonable endeavours to promptly resolve such matter.

3.2 In the event that a third party T Level Awarding Organisation contends that it is unable to meet its joint arrangement obligations as a result of the action or inaction of the Supplier, then the Supplier shall comply with the reasonable instructions of the Authority in relation to such action or inaction.

3.3 Nothing in this Schedule (including any failure to agree any matters referred to in paragraph 2 of this Schedule) shall operate to reduce or otherwise diminish the Supplier's obligations and/or the Authority's rights under this Contract.

4 Reporting

4.1 The Supplier shall, on request by the Authority, promptly provide a written report to the Authority setting out its progress in achieving the joint arrangements set out in paragraph 2 of this Schedule.

Schedule 5

Supplier's Response

The content for this Schedule is contained in separate files at.

S5_GEN2W1_DSS_Risk_Register

S5_GEN2W1_DSS_AQ9.1-10.7_Supplier_Responses

S5_GEN2W1_DSS_Q9.5_Grading_and_Awarding_Structure

S5_GEN2W1_DSS_Q10.4_Internal_Quality_Assurance_Process

S5_GEN2W1_DSS_Q10.7_Management_and_Governance

S5_GEN2W1_DSS_Q10.7_Escalation_Process_Flow

S5_GEN2W1_DSS_Issues_Log

S5_GEN2W1_Clarifications

Schedule 5

Risk Register

S5_GEN2W1_DSS_Q10.1_TQ_Risk_Register

Schedule 5

Supplier Responses

S5_GEN2W1_DSS_AQ9.1 - Q10.7_Supplier_Responses

Schedule 5

Awarding Structure

S5_GEN2W1_DSS_Q9.5_Grading_and_Awarding_Structure

Schedule 5

Internal Quality Assurance Process

S5_GEN2W1_DSS_Q10.4_Internal_Quality_Assurance_Process

Schedule 5

Management and Governance

S5_GEN2W1_DSS_Q10.7_Management_and_Governance

Schedule 5

Escalation Process Flow

S5_GEN2W1_DSS_Q10.7_Escalation_Process_Flow

Schedule 5

Issues Log

S5_GEN2W1_DSS_Q10.7_Issues_log

Schedule 5

Clarifications

S5_GEN2W1_DSS_Clarifications

Schedule 6

Pricing Schedule

The content for this Schedule is contained in a separate file at:

S6_GEN2W1_DSS_Pricing_Schedule

Award Questionnaire Q10.5: Financial Capacity - Instructions

Introduction

The following tab is designed for Potential Suppliers to complete the financial forecast for question 10.5, as requested in 'ITT Attachment 6 part 3 - Award Questionnaire Lot-specific questions', aiming to assess financial capacity of Potential Suppliers. This does not form part of the Tender pricing process or pricing evaluation process. Please note that no price impacting assumptions or caveats will be accepted within a Tender. Note the separate instructions relating to the Pricing Schedule which must also be followed.

How to complete this question

Potential Suppliers must complete and submit one copy of this answer for each TQ (ie a separate response for each Lot they intend to submit a Tender for).

The following tab is designed for Potential Suppliers to complete the financial forecast for question 10.5, as requested in 'ITT Attachment 6 part 2 - Award Questionnaire'.

>> Q10.5 Attachment Template: Potential Suppliers must complete all boxes coloured yellow (in columns F to N) of the Q10.5 Attachment Template tab. Values should be entered in £ pounds sterling and rounded to the nearest pound. Please note this can be with a 0 value. Values should exclude any applicable VAT. Where further explanation is required, please use the free text 'comments' boxes in column Q to provide this.

As stated in question 10.5, the attachment requests the Potential Supplier's financial forecast for delivery of the Services under the Contract. This includes the sources of income relating to the Services and the anticipated spend per year in the delivery of the Services over the Contract term. The financial forecast should include a level of detail that enables the Authority to assess the basis and reasonableness of the calculations. In the template, the sources of income are listed as a Qualification Refresh charge, Entry Fees, Additional Services fees, and any charges for Exclusive TQ Changes. The definitions for these are as listed in the Pricing Schedule 'Instructions 1' tab or defined in the Contract. Categories for the relevant fixed and variable costs have been suggested in the template. If there are any missing, please add the relevant figures under 'other' stating what the new categories are.

Potential Suppliers should complete a breakdown of their anticipated spend on sub-contracting elements of the Services, by sub-contractor. If you do not intend to use sub-contractors, you do not need to complete this section. The figures entered here should represent the annual cost to the Potential Supplier of sub-contracting the relevant elements of the Services under the Contract and should therefore represent a proportion of the Potential Supplier's total anticipated annual costs. The relevant sub-contracting costs should also be included in the figures entered separately against the relevant fixed and variable cost categories listed above. Potential Suppliers must provide the sub-contracting breakdown against their two key sub-contractors (if there are multiple sub-contractors) and then include separately any costs in respect of anticipated spend with any other sub-contractors. Please list the highest value sub-contracted Services first.

The financial forecast is not binding on Potential Suppliers.

Further notes

Assumptions – Solely for the purposes of provision of the financial forecast, Potential Suppliers are encouraged to use their own estimates of key volume variables (i.e. Student numbers and take up of Additional Services) rather than those provided as estimates in this Pricing Schedule, if different. Suppliers should include their own best estimate of income and costs associated with each element. Potential Suppliers will however be expected to complete the financial forecast on the basis of the prices quoted in the Pricing Schedule on tab 'Input A' for the Qualification Refresh charge, entry fees and Additional Services fees.

Definitions – For each fee area, definitions are as those outlined on the 'Instructions 1' tab of the Pricing Schedule or defined in the Contract.

Inflation – Any impact of inflation should not be included in the template - i.e. Potential Suppliers should complete the financial forecast template assuming zero inflation throughout the Contract term.

Schedule 6A

Adaptive Pricing

1. The Review Triggers

1.1 The Parties agree that the Entry Fee, as referred to in Schedule 6, shall be reviewed and may change, in the following two instances:

1.1.1 in or around [December 2026], which shall be referred to as the Mid-Term Review; and

1.1.2 in the event that the Authority seeks to extend the Contract in accordance with clause 2.2 and 15.2 of the Contract, in or around [December 2028], which shall be referred to as the Extension Review.

2. The Mid Term Review

2.1 On or around [1st December 2026] the Authority shall provide the Supplier with an updated projection of total learner volumes for the five Exclusive Cohorts under the Contract which shall be referred to as the Updated Projection.

2.2 The Updated Projection shall be calculated by the Authority by combining the actual learner volumes for Exclusive Cohorts one and two, as confirmed by the Department to the Authority, with the revised estimates for the remaining three Exclusive cohorts of the Contract, as determined by the Department and confirmed to the Authority.

Circumstances in which an Enhanced Entry Fee is permitted

2.3 Where the Updated Projection is calculated to be at least 15% less than the total learner volume contained in the original tender documents, which shall be referred to as the Initial Projection, the Authority shall determine a revision to the Entry Fee which shall be referred to as the Enhanced Entry Fee and will be in such amount as to enable the Supplier to retain the opportunity to achieve its % profit margin, as set out in Schedule 6, over the life of the original Contract and;

2.3.1 the Authority shall notify the Supplier in writing, on or before the [31st December 2026] of the Enhanced Entry Fee;

2.3.2 by no later than the end of February in the Academic Year prior to the Academic Year in which the Enhanced Entry Fee may be applied the Supplier shall notify the Authority in writing of its intention to substitute the Entry Fee with the Enhanced Entry Fee, or such other Entry Fee not exceeding the Enhanced Entry Fee, as the case may be;

2.3.3 for the avoidance of doubt, any Entry Fee to be adopted by the Supplier pursuant to the provisions of this paragraph 2.3, will also incorporate any adjustments proposed by the Supplier under clause 4.12 of the Contract. The collective adjustments calculated in accordance with this paragraph 2.3 and or clause 4.12 will not exceed the Enhanced Entry Fee.

2.3.4 Any Enhanced Entry Fee shall apply for the Cohort for the Academic Year commencing 1 August [2027] and shall continue to apply to the Cohort for the Academic Year commencing 1 August [2027] and the Cohort for the Academic Year commencing 1 August [2027], and may be subject to later adjustments effected by the further application of clause 4.12 of the Contract.

Circumstances in which a Reduced Entry Fee will be required

2.4 Where the Updated Projection is calculated to be at least 15% more than the Initial Projection, the Authority shall determine a reduced Entry Fee which shall be referred to as the Reduced Entry Fee which will be in such amount as to enable the Supplier to retain the opportunity to achieve, but not exceed, its % profit margin, as set out in Schedule 6.

2.4.1 The Authority shall notify the Supplier in writing, on or before the [31st December 2026] of the Reduced Entry Fee;

2.4.2 For the avoidance of doubt, the Reduced Entry Fee will also incorporate any adjustments proposed by the Supplier under clause 4.12 of the Contract.

2.4.3 The Reduced Entry Fee shall apply for the Cohort for the Academic Year commencing 1 August [2027] and shall apply to the Cohort for the Academic Year commencing 1 August [2027] and the Cohort for the Academic Year

commencing 1 August [20xx], and may be subject to later adjustments effected by the further application of clause 4.12 of the Contract.

3. The Extension Review

3.1 In the event of notification by the Authority to the Supplier of their intention to extend the Contract in accordance with clause 2.2 and 15.2, which shall be referred to as 'the First Extension Period', the Authority shall:

3.1.1 before the end of the final Exclusive Cohort, provide the Supplier with the projection of learners for the Academic Years which fall within the First Extension Period following the end of the fifth Exclusive Cohort, as determined by the Department and confirmed to the Authority, which shall be referred to as the Final Updated Projection;

3.1.2 where the Final Updated Projection is calculated to be at least 15% less than the Updated Projection for the fifth Exclusive Cohort, calculate the Entry Fee applicable to the First Extension which shall be referred to as the Extension Entry Fee, in such a sum which ensures that the Supplier retains the opportunity to achieve its % profit margin, as set out in Schedule 6, during the First Extension Period;

3.1.3 the Authority shall notify the Supplier in writing, on or before the [31st December 2028] of the Extension Entry Fee;

3.1.4 by no later than the end of February in the Academic Year prior to the Academic Year in which the Extension Entry Fee may be applied the Supplier shall notify the Authority in writing of its intention to substitute the Entry Fee with such other Entry Fee not exceeding the Extension Entry Fee, as the case may be;

3.1.5 the Extension Entry Fee shall also incorporate any adjustments to the Entry Fee effected by the application of clause 4.12;

3.1.6 any Extension Entry Fee shall apply for the Cohorts for the Academic Years which fall within the First Extension Period.

3.2 In the event that the Authority seeks to extend the Contract beyond the First Extension Period, in accordance with the provisions of clause 2.2 and 15.2 of the Contract, the Extension Entry Fee shall not be amended further save for any adjustments effected by the application of clause 4.12.

Circumstances in which a Reduced Extension Entry Fee will be required

3.3 Where the Final Updated Projection is calculated to be at least 15% more than the Updated Projection for the fifth Exclusive Cohort, the Authority shall determine a reduced Entry Fee which shall be referred to as the 'Reduced Extension Entry Fee' which will be in such amount as to enable the Supplier to retain the opportunity to achieve, but not exceed, its % profit margin, as set out in Schedule 6.

3.3.1 The Authority shall notify the Supplier in writing, on or before the [31st December 2028] of the Reduced Extension Entry Fee;

3.3.2 For the avoidance of doubt, the Reduced Extension Entry Fee will also incorporate any adjustments proposed by the Supplier under clause 4.12 of the Contract.

3.3.3 The Reduced Extension Entry Fee shall apply for the Cohorts for the Academic Years which fall in with the First Extension Period, and may be subject to later adjustments effected by the further application of clause 4.12 of the Contract.

4. General

4.1 The Authority does not provide any assurance that the Updated Projection will be achieved and the Supplier bears all risks arising from any variance between the Updated Projection, the Final Updated Projection and the actual learner volumes that emerge through the life of the contract.

Schedule 7

Staff (including Key Personnel)

1 Key Personnel

1.1 The Supplier shall ensure that the Key Personnel fulfil the Key Roles during the Term. The Annex to this Schedule 7 lists the Key Roles. remit and names of the persons who the Supplier shall appoint to fill those Key Roles at the Effective Date.

1.2 The Authority can identify any further roles as being Key Roles and, following agreement on this by the Supplier (such agreement not to be unreasonably withheld or delayed) any relevant person selected to fill those Key Roles (and details of the role itself) shall be included on the list of Key Personnel in the Annex to this Schedule 7.

1.3 The Supplier shall not remove or replace any Key Personnel (including when carrying out its obligations under Schedule 12 (*Exit Management*)) unless:

1.3.1 requested to do so by the Authority;

1.3.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave;

1.3.3 the person's employment or contractual arrangement with the Supplier or a Subcontractor is terminated for material breach of contract by the employee; or

1.3.4 the Supplier obtains Approval (such Approval not to be unreasonably withheld or delayed).

1.4 The Supplier shall:

1.4.1 notify the Authority promptly of the absence of any Key Personnel (other than for short-term sickness or holidays of 2 weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.4.2 ensure that any Key Role is not vacant for any longer than 10 Working Days;

1.4.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Personnel and, except in the cases of death,

unexpected ill health or a material breach of the Key Personnel's employment contract, this will mean at least 60 Working Days' notice;

1.4.4 ensure that all arrangements for planned changes in Key Personnel provide adequate periods during which incoming and outgoing personnel work together to transfer responsibilities and ensure that such change does not have an adverse impact on the performance of the Services and/or supply of any Products; and

1.4.5 ensure that any replacement for a Key Role:

(i) has a level of qualifications and experience appropriate to the relevant Key Role; and

(ii) is fully competent to carry out the tasks assigned to the Key Personnel whom he or she has replaced.

2 Staff vetting

2.1 For the purposes of this paragraph 2, "**Convictions**" means, other than in relation to minor road traffic offences, any previous or pending prosecutions, convictions, cautions and binding-over orders (including any spent convictions as contemplated by section 1(1) of the Rehabilitation of Offenders Act 1974 or any replacement or amendment to that Act).

2.2 The Supplier shall ensure that all potential Supplier Staff or persons performing any of the Services during the Term who may reasonably be expected in the course of performing any of the Services under this Contract to have access to or come into contact with Students or vulnerable persons (and/or access to data or information relating to such Students or vulnerable persons) are, to the extent permitted by Law:

2.2.1 questioned concerning their Convictions; and

2.2.2 required to obtain appropriate disclosures from the Disclosure and Barring Service (or other appropriate body) where required by Law,

before the Supplier engages the potential staff or persons in the provision of the Services.

2.3 The Supplier shall take all necessary steps to ensure that such potential staff or persons referred to in paragraph 2.2 obtain standard and enhanced disclosures from the Disclosure and Barring Service (or other appropriate body) and shall ensure all such disclosures are kept up to date. The obtaining of such disclosures shall be at the Supplier's cost and expense.

2.4 The Supplier shall ensure that no person is employed or otherwise engaged in the provision of the Services without the Authority's prior written consent if:

2.4.1 the person has disclosed any Convictions upon being questioned about their Convictions in accordance with paragraph 2.2.1;

2.4.2 the person is found to have any Convictions following receipt of standard and/or enhanced disclosures from the Disclosure and Barring Service (or other appropriate body) in accordance with paragraph 2.2.2; or

2.4.3 the person fails to obtain standard and/or enhanced disclosures from the Disclosure and Barring Service (or other appropriate body) upon request by the Supplier under paragraph 2.2.2.

2.5 In addition to the requirements of paragraphs 2.1 to 2.4, where the Services are or include regulated activities as defined by the Safeguarding Vulnerable Groups Act 2006 the Supplier shall:

2.5.1 comply with all requirements placed on it by the Safeguarding Vulnerable Groups Act 2006;

2.5.2 ensure that it has no reason to believe that any member of Supplier Staff is barred in accordance with the Safeguarding Vulnerable Groups Act 2006; and

2.5.3 ensure that no person is employed or otherwise engaged in the provision of the Services if that person is barred from carrying out, or whose previous conduct or records indicate that they would not be suitable to carry out, any regulated activities as defined by the Safeguarding Vulnerable Groups Act 2006 or may present a risk to Students or any other person.

2.6 The Supplier shall ensure that the Authority is kept advised at all times of any member of the Supplier Staff who, subsequent to their commencement of employment as a

member of the Supplier Staff receives a Conviction or whose previous Convictions become known to the Supplier or whose conduct or records indicate that they are not suitable to carry out any regulated activities as defined by the Safeguarding Vulnerable Groups Act 2006 or may present a risk to Students or any other person. The Supplier shall only be entitled to continue to engage or employ such individual with the Authority's written consent and with such safeguards being put in place as the Authority may reasonably request. Should the Authority withhold consent the Supplier shall immediately remove such individual from the Supplier Staff.

2.7 The Supplier shall immediately provide to the Authority any information that the Authority reasonably requests to enable the Authority to satisfy itself that the obligations set out in paragraphs 2.1 to 2.6 of this Schedule have been met.

2.8 For Supplier Staff appointed following the Effective Date who shall or may have access to IfATE Data, in addition to meeting its obligations under this paragraph 2, the Supplier shall carry out pre-employment screening meeting the HMG Baseline Personnel Security Standard (BPSS) or equivalent in accordance with Schedule 9 (*Data Handling and Security Management*).

Annex to Schedule 7

List of Key Personnel

The content for this Annex is contained in a separate file at:

S7_A1_GEN2W1_DSS_List_of_Key_Personnel

Schedule 8

Supply Chain (including approved Subcontractors)

1 Appointment of Key Subcontractors

1.1 Where the Supplier wishes to enter into a Key Sub-Contract or replace a Key Subcontractor, it must obtain Approval, such Approval not to be unreasonably withheld or delayed. For these purposes, the Authority may withhold its Approval to the appointment of a Key Subcontractor if it reasonably considers that:

1.1.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Services and/or the supply of the Products or may be contrary to the interests of the Authority and/or the TQ;

1.1.2 the proposed Key Subcontractor is unreliable and/or has not provided reasonable services to its other customers or clients;

1.1.3 the proposed Key Subcontractor employs unfit persons; or

1.1.4 the proposed Key Subcontractor should be excluded in accordance with clause 15.715.8 (*Ending or extending this Contract*).

1.2 The Authority confirms its Approval of the appointment of the Key Subcontractors listed in Annex 1 to this Schedule 8.

1.3 Except where the Authority has given its Approval otherwise, the Supplier shall ensure that each Key Sub-Contract shall include:

1.3.1 provisions which will enable the Supplier to discharge its obligations under this Contract;

1.3.2 a right for the Authority to enforce any provisions under the Key Sub-Contract which are capable of conferring a benefit upon the Authority;

1.3.3 a provision enabling the Authority to enforce the Key Sub-contract as if it were the Supplier;

1.3.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to the

Authority or any Replacement Supplier without restriction (including any need to obtain any consent or approval) or payment by the Authority; and

1.3.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Contract:

(i) under clauses 18.1 to 18.9.4 (*Data protection and information*);

(ii) under clause 20 (*When information can be shared*);

(iii) in respect of any obligation not to bring the Authority, the Department or the ESFA and/or the T Levels Programme into disrepute and/or otherwise diminish the trust that the public places in the Authority, the Department or the ESFA, as set out in clause 3.1.9 (*How the Services must be supplied*); and

(iv) in respect of the keeping of records and provision of information (including (as applicable) Management Information) in relation to that part of the Services being provided and/or those Products being supplied under the Key Sub-Contract.

1.4 The Supplier shall, as soon as reasonably practicable following a request by the Authority, provide a copy of any proposed Key Sub-Contract (and/or any Key Sub-Contract which it has entered into) to demonstrate compliance by the Supplier with its obligations under this paragraph 1.

2 <u>Subcontractor information</u>

2.1 If the Authority asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

2.1.1 their name;

2.1.2 the scope of their appointment; and

2.1.3 the duration of their appointment.

Annex 1 to Schedule 8

Key Subcontractors

Not Used

Schedule 9

Data Handling and Security Management

1 The Supplier shall maintain Cyber Essentials certification and shall operate an Information Security Management System in relation to the Services that is compliant with ISO 27001 (the International Standard for Information Security Management Systems) or an equivalent standard.

2 The Supplier shall have in place and maintain physical security, in line with the requirements outlined in ISO 27002 (the International Standard describing the Code of Practice for Information Security Controls), including entry control mechanisms (e.g. door access) to premises and sensitive areas.

3 The Supplier shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to IT systems to ensure only authorised personnel have access to IfATE Data.

4 The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect IfATE Data, including: physical security controls; Good Industry Practice policies and processes; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions, operating systems, network devices and application software; user access controls; and the creation and retention of audit logs of system use.

5 The Supplier shall carry out and shall maintain records of appropriate technical risk assessments in respect of all aspects of the Supplier's handling of IfATE Data. The Supplier shall provide such records to the Authority on request and shall ensure that such records are capable of demonstrating to the Authority's reasonable satisfaction that appropriate procedures are in place to address any significant risks identified.

6 The Supplier shall ensure that IfATE Data is processed and stored in a manner which enables such IfATE Data to be identified and securely deleted when required. The Supplier shall ensure that IfATE Data which is not in electronic form is kept physically separate from the data of the Supplier and any of the Supplier's other customers.

7 Any IfATE Data transferred by the Supplier using electronic transfer methods across public space or cyberspace, including mail and courier systems, or third party provider

networks must be encrypted to an encryption standard meeting Transport Layer Security (TLS) 1.2 or later.

8 Storage of IfATE Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated requirement and shall be subject to paragraphs 9 and 10 below.

9 Any portable removable media (including pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process IfATE Data to deliver or support the Services, shall be under the control and configuration management of the Supplier, shall be necessary to deliver the Services and shall be encrypted to the Advanced Encryption Standard (AES) 256 or equivalent.

10 All portable IT devices (including laptops, tablets, smartphones or other devices, such as smart watches) which handle, store or process IfATE Data to deliver and support the Services, shall be under the control and configuration management of the Supplier, shall be necessary to deliver the Services and shall be full-disk encrypted to the Advanced Encryption Standard (AES) 256 or equivalent.

11 Whilst in the Supplier's care, all removable media and hardcopy paper documents containing IfATE Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder, a professional secure disposal organisation or an equivalent secure disposal method.

12 When necessary to hand-carry removable media and/or hardcopy paper documents containing IfATE Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of the Supplier's premises.

13 The Supplier shall ensure throughout the Term that it is in a position (and is able to demonstrate to the Authority's reasonable satisfaction that it is in a position) to provide a complete copy of all IfATE Data at the Authority's request at any time and on the termination or expiry of the Contract.

14 At the end of the Contract or in the event of equipment failure or obsolescence, all IfATE Data, in either hardcopy or electronic format, that is physically held or logically stored on the Supplier's IT infrastructure must be securely sanitised or destroyed and accounted for in a manner that ensures that the relevant data is not retrievable using normally available methods and/or tools and which allows the Supplier to demonstrate its compliance with this paragraph 14 at the Authority's request. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, then the Supplier shall protect the Authority's information and data until such time that it can be securely cleansed or destroyed.

15 Access by Supplier Staff to IfATE Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role and have undergone pre-employment screening appropriate to the nature and sensitivity of the IfATE Data and, for Supplier Staff appointed following the Effective Date, have undergone pre-employment screening which is at least equivalent to the HMG Baseline Personnel Security Standard (BPSS).

16 All Supplier Staff who handle IfATE Data must have annual awareness training in protecting information.

17 The Supplier shall have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures to ensure that the delivery of the Services is not adversely affected in the event of an incident (as set out in the Supplier's Business Continuity Plan). An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the Services. Upon request from the Authority, the Supplier will provide evidence of the effectiveness of their business continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

18 Any suspected or actual breach of the confidentiality, integrity or availability of IfATE Data being handled in the course of providing the Services, or any non-compliance with security standards pertaining to the Services, shall be investigated immediately and escalated to the Authority. The Supplier shall maintain audit records and event logs in respect of any such security events in accordance with documented retention policies approved by the Authority.

19 The Supplier shall ensure that any IT systems and hosting environments that are used to handle, store or process IfATE Data shall be subject to independent penetration testing, to take place within the three month period immediately prior to the start of each Academic Year, to test the security of such systems and hosting environments, by a penetration testing provider that is CHECK, CREST or TIGER scheme approved. The Supplier shall include a summary of the findings of such penetration testing and the details of any necessary remedial work carried out in the annual penetration testing report required under Schedule 2 (*Service Requirements*). In the event of security issues being identified which are ranked as "high" importance or above, the Supplier shall notify the Authority as soon as reasonably possible (and in any event within 2 Working Days), shall promptly remedy such issues, and shall promptly carry out a follow-up remediation test at the Authority's request.

20 The Supplier shall ensure that any consumer-off-the-shelf software used in relation to the IfATE Data or otherwise to deliver the Services is kept up-to-date and subject to mainstream support.

21 The Supplier shall procure and implement security patches to address any vulnerabilities in the IT systems used to handle the IfATE Data or to deliver the Services, within a period of time appropriate to the risk the vulnerability presents.

22 The Supplier shall not without the prior written agreement of the Authority store any IfATE Data outside of the UK or perform any form of IT management, support or development function from outside the UK. The Supplier shall provide the Authority with full details of any proposal to do so and shall not go ahead with any such proposal without the prior written agreement of the Authority.

23 The Supplier shall undergo appropriate security assurance activities as may reasonably be determined by the Authority from time to time and shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation. This will include obtaining any necessary professional security resources required to support the Supplier's security assurance activities.

24 The Supplier shall have in place and maintain a secure system for data exchange sufficient to enable the Supplier to make all required Management Information and Ofqual information returns in relation to the TQ and the Services.

25 Unless otherwise agreed in writing by the Authority, the Supplier shall ensure that any of their Subcontractors, third party suppliers or partners (including any Assessor who is self-employed or who provides services to the Supplier through that Assessor's own personal service company) who could potentially access any IfATE Data meet all of the requirements in this Schedule as they apply to the Supplier and shall contractually enforce such requirements onto any such Subcontractors, third party suppliers or partners (including any Assessor who is self-employed or who provides services to the Supplier through that Assessor's own personal service company).

Schedule 10

Business Continuity

The content for this Schedule is contained in a separate file at:

S10_GEN2W1_DSS_Business_Continuity

Schedule 11

Change Management

Variation Form

Variation Form / change control note (CCN) No:	**Contract:**	**Effective Date of Variation:**
Initiated by: Change requested by [Supplier **OR** Authority]		
Date of request:		
Period of validity: This Variation Form is valid for acceptance until [DATE].		
Reason for change:		
Description and impact of the change (including to delivery and performance):		
Time limit for Impact Assessment:		
Required amendments to wording of Contract or Schedules:		
Adjustment to Charges resulting from change:		
Supporting or additional information:		

SIGNED ON BEHALF OF THE AUTHORITY	**SIGNED ON BEHALF OF THE SUPPLIER**
Signature:	Signature:
Name:	Name:
Position:	Position:
Date:	Date:

Schedule 12

Exit Management

PART A: GENERAL

1 Exit Plan

1.1 The Supplier shall, within two Months after the Effective Date, deliver to the Authority an initial Exit Plan (adopting and updating the form of plan at Annex 1 to this Schedule 12) that:

1.1.1 sets out the Supplier's proposed methodology for achieving an orderly transfer of the Services to the Authority and/or its Replacement Supplier on the expiry or termination of this Contract;

1.1.2 complies with the requirements set out in paragraph 1.3 below; and

1.1.3 is otherwise reasonably satisfactory to the Authority.

1.2 The Authority shall consider the initial Exit Plan and shall notify the Supplier of any amendments it believes are necessary. The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 30 Working Days of the Authority requesting any amendments, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

1.3 The Exit Plan shall set out, as a minimum:

1.3.1 how the Exit Information will be obtained;

1.3.2 separate mechanisms for dealing with Ordinary Exit, Early Exit and Emergency Exit, with the provisions relating to Early Exit and Emergency Exit prepared on the assumption that the Supplier may be unable to provide the full level of assistance that is required by the provisions relating to Ordinary Exit, and to include in the case of Early Exit and Emergency Exit, provision for the supply by the Supplier of all such reasonable assistance as the Authority shall require to enable the Authority or its sub-contractors to provide the Services;

1.3.3 the management structure to be employed during the transfer of the Services in the event of each of an Ordinary Exit, an Early Exit and an Emergency Exit;

1.3.4 a detailed description of the transfer processes, including a timetable, applicable in the case of each of an Ordinary Exit, an Early Exit and an Emergency Exit;

1.3.5 steps the Supplier will take to mitigate the potential for and/or costs of any redundancies (if applicable) of any individual employed by either the Supplier or any Subcontractor in the provision of the Services in the event of each of an Ordinary Exit, an Early Exit and an Emergency Exit; and

1.3.6 without prejudice to the Supplier's obligations elsewhere in this Schedule, the scope of any further termination-related assistance that may reasonably be required by the Authority to achieve an orderly transfer of the Services to the Authority and/or its Replacement Supplier in the case of each of an Ordinary Exit, an Early Exit, and an Emergency Exit.

2 Updates to the Exit Plan

2.1 The Supplier shall review and (if appropriate) update the Exit Plan:

2.1.1 following IfATE Approval;

2.1.2 at least once every Academic Year;

2.1.3 whenever there is a material change to the Services (including any TQ Change); and

2.1.4 within 10 Working Days of the service of a Termination Notice,

and consider what changes (if any) are necessary to reflect the current state of the Services and the TQ at the relevant point in time and to ensure that the Exit Plan meets the requirements of this Schedule and is capable of being implemented promptly.

2.2 Following each review required under paragraph 2.1, the Supplier shall submit for the Authority's approval a revised draft of the Exit Plan showing any proposed amendments necessary to ensure the Exit Plan continues to meet the requirements of this Schedule. The Authority shall consider each such revised draft and shall notify the

Supplier of any further amendments it believes are necessary. The Supplier shall incorporate all reasonable amendments requested by the Authority in a further revised draft of the Exit Plan. If the Parties are unable to agree the contents of a revised Exit Plan within 30 Working Days of the Authority requesting any amendments, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.3 When the revised Exit Plan is agreed, it shall be signed by both Parties, following which it shall supersede any previous versions of the Exit Plan.

3 Provision of Exit Information

3.1 The Supplier shall provide to the Authority the Exit Information (as defined in paragraph 3.2 below) in an appropriate documentary form:

3.1.1 within one Month of the date 12 Months prior to the Expiry Date (as extended by any Extension Period);

3.1.2 as soon as reasonably practicable after (and in any event within one Month of) the date of service of a Termination Notice by either Party; and

3.1.3 at the Authority's request on reasonable notice at any point during the Term provided that the Authority shall not make such a request more than twice in any 6 month period.

3.2 Subject to paragraph 3.3, the information to be provided under paragraph 3.1 shall include all such information as is reasonably necessary and sufficient to enable the Authority and/or any Replacement Supplier to take over and provide the Services and the TQ following the expiry or termination of this Contract (the "**Exit Information**"), and in particular shall include:

3.2.1 details of all Supplier third party contracts or licences used for the provision of the Services (including any Transferable Contracts) including, where applicable, whether such contracts or licences are used by the Supplier to provide services to other customers of the Supplier, save to the extent these details are subject to an obligation of confidence to a third party that is not part of the Supplier's corporate group;

3.2.2 details of all the Intellectual Property Rights used in the provision of the Services or developed as part of the Services;

3.2.3 details of any IfATE Data that is in the possession or control of the Supplier or any Subcontractors or that is otherwise used in the provision of the Services;

3.2.4 details of any Key Materials and Ancillary Materials;

3.2.5 details of any ongoing projects or other work carried out under this Contract; and

3.2.6 in respect of all individuals engaged in providing the Services, such information as the Authority may reasonably request (subject, at all times, to any relevant Data Protection Legislation), including in an anonymised format full and accurate details of:

(i) the total number of such individuals;

(ii) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;

(iii) their dates of commencement of employment or engagement;

(iv) their remuneration and other benefits;

(v) their other terms and conditions of employment, as applicable (including their relevant contractual notice periods and any other terms relating to termination of employment, redundancy procedures and redundancy payments);

(vi) their job titles and job descriptions;

(vii) details of any such individuals on long term sickness absence, parental leave, maternity leave, paternity leave or other authorised long-term absence;

(viii) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);

(ix) details of who reports to each individual and to whom each individual reports; and

(x) any collective agreements that apply to them; and

3.2.7 any other material or information reasonably requested by the Authority.

3.3 The Supplier shall not be required to provide in the Exit Information any information that has already been provided to the Authority as part of the Management Information, unless that information has become outdated and/or inaccurate since it was last provided as part of the Management Information.

3.4 Once provided in accordance with paragraph 3.1 above, the Supplier shall provide any updates to the Exit Information to the Authority:

3.4.1 on a Monthly basis (following any Month where there are changes to the Exit Information) following the earliest of the dates referred in to paragraphs 3.1.1 and 3.1.2; and

3.4.2 as soon as reasonably practicable following (and in any case within one Month of) the Authority's reasonable request, provided that the Authority shall not make such a request more than twice in any 6 Month period.

3.5 The Exit Information shall be deemed to be Confidential Information. The Authority shall only use the Exit Information for the Exit Purposes as defined in paragraph 4.2 below, and shall ensure that such Exit Information is only disclosed within the Authority to those individuals who need to know the Exit Information for the Exit Purposes. The Authority may disclose the Exit Information to any Replacement Supplier for the Exit Purposes.

4 Provision of assistance on termination or expiry

4.1 In connection with any expiry or termination of this Contract for whatever reason, the Parties shall perform their respective obligations as stated in the Exit Plan, and without prejudice to the generality of this obligation:

4.1.1 the Supplier shall provide to the Authority and/or any Replacement Supplier (as applicable) all reasonable assistance requested by the Authority for the transfer of the Services and the TQ from the Supplier to the Authority and/or the Replacement Supplier (as applicable) with the minimum of disruption and inconvenience to Students and Stakeholders;

4.1.2 the Supplier shall provide the Authority with:

(i) a complete copy of all Key Materials;

(ii) a complete copy of any Ancillary Materials that have not previously been provided or that have been updated since they were last provided; and

(iii) at the Authority's request, further copies of any Ancillary Materials previously provided;

4.1.3 the Supplier shall provide the Authority or, at the Authority's request, any Replacement Supplier, with a copy of all IfATE Data that is in the possession or control of the Supplier or any Subcontractors or that is otherwise used in the provision of the Services;

4.1.4 the Supplier shall provide any additional information reasonably required by the Authority to understand and access any data or information provided by the Supplier; and

4.1.5 at the Authority's request, the Supplier shall enter into a period of parallel running of the Services alongside the running of any Replacement Services and shall use its reasonable endeavours to facilitate a phased transfer of the Services to the Authority and/or any Replacement Supplier (but only where that phased transfer does not impact on the Supplier's ability to deliver the Services that it remains responsible for providing under this Contract).

4.2 Without prejudice to the terms of clause 13 (*Intellectual Property Rights*), the Supplier hereby grants to the Authority a worldwide, royalty free licence (with a right to sublicense to any Replacement Supplier) to use any information, data, software or materials referred to in the Exit Information or provided by the Supplier or its Subcontractors in the performance of the Supplier's obligations under this paragraph 4. The Authority and any Replacement Supplier sub-licensees may only use such information, data, software and materials for such purposes and for such period as is reasonably necessary to ensure an orderly transfer of the Services to the Authority or a Replacement Supplier that minimises disruption and inconvenience to Students and Stakeholders ("**Exit Purposes**").

4.3 In the event of an Emergency Exit, the Supplier shall grant or procure the grant to the Authority and any Replacement Supplier the right during any Transition Period and on termination of this Contract to access and use the IT systems used by the Supplier (including software and databases) insofar as such access and use is necessary in order to enable an orderly transfer of the Services to the Authority and/or its Replacement Supplier on the termination of this Contract, and the Supplier shall provide such access, information and credentials as are required for the Authority and/or Replacement Supplier to access such systems for such purposes.

5 Transferable Contracts

5.1 During the period beginning 6 Months prior to the End Date or following the service of a Termination Notice by either party, the Supplier shall not without the Authority's prior written consent terminate, enter into or vary:

5.1.1 any Transferable Contract; or

5.1.2 any other Sub-Contract, except to the extent such change does not or will not affect the provision of the Services or the Charges.

5.2 On expiry or termination of this Contract for any reason, the Supplier shall at the Authority's request assign, novate or procure the novation of the Supplier's interest in the Transferable Contracts to the Authority or a Replacement Supplier.

6 Costs of assistance on termination or expiry

6.1 Save in respect of the provision of the Services (for which the Supplier shall continue to be remunerated in accordance with Schedule 6 (*Pricing Schedule*)):

6.1.1 where the Contract is terminated by the Authority as a result of a Supplier Termination Event under clause 15.3 (*Ending or extending this Contract*) or where the Contract is wrongfully terminated or repudiated by the Supplier, the Parties' costs of compliance with paragraph 4 shall be borne by the Supplier; and

6.1.2 where the Contract is terminated by the Supplier under clause 15.5 (*Ending or extending this Contract*) or where the Contract is wrongfully terminated or repudiated by the Authority, the Parties' costs of compliance with paragraph 4 shall be borne by the Authority.

6.2 References to "**costs**" in paragraph 6.1 shall be deemed to refer only to direct, reasonable and verifiable costs (which, in the case of the Supplier, shall be calculated in accordance with the Rate Card). Both Parties shall use all reasonable endeavours to mitigate such costs and, to the extent reasonably practicable, each Party shall notify and obtain the consent of the other Party before incurring any costs for which the other Party would be liable under paragraph 6.1.

6.3 Subject to paragraph 6.1, each Party shall bear its own costs of compliance with this Schedule.

7 General

7.1 The Supplier warrants to the Authority that all the information provided under paragraphs 3 and 4 shall conform to the requirements of this Contract or, where there are no such requirements, shall be prepared in accordance with Good Industry Practice.

7.2 Except as otherwise stated in the Exit Plan:

7.2.1 the obligations in paragraphs 4 and 5 shall be in addition to, and not in substitution for, the provision of the Services; and

7.2.2 subject to the continued payment of the Charges in accordance with the terms of this Contract, the Supplier shall continue to provide, and the Authority shall continue to receive, the Services during the Term in accordance with the terms and conditions of this Contract.

PART B: EMPLOYMENT

8 Employment exit provisions

8.1 This Contract envisages that subsequent to its commencement, the identity of the provider of the Services (or any part of the Services) may change (whether as a result of termination of this Contract, or part or otherwise) resulting in a transfer of the Services in whole or in part ("**Subsequent Transfer**"). If a Subsequent Transfer is a Relevant Transfer then the Authority or Replacement Supplier will inherit liabilities in respect of the Relevant Employees with effect from the Relevant Transfer Date.

8.2 The Supplier shall and shall procure that any Subcontractor shall on receiving notice of termination of this Contract or otherwise, on request from the Authority and at such times as required by TUPE, provide in respect of any person engaged or employed by the Supplier or any Subcontractor in the provision of the Services, the Supplier's Provisional Supplier Personnel List and the Staffing Information together with any additional information required by the Authority, including information as to the application of TUPE to each individual listed on the Supplier's Provisional Supplier Personnel List. The Supplier shall notify the Authority of any material changes to this information as and when they occur.

8.3 At least 28 days prior to the Relevant Transfer Date, the Supplier shall and shall procure that any Subcontractor shall prepare and provide to the Authority and/or, at the direction of the Authority, to the Replacement Supplier, the Supplier's Final Supplier Personnel List, which shall be complete and accurate in all material respects. The Supplier's Final Supplier Personnel List shall identify which of the Supplier's and Subcontractor's personnel named are Relevant Employees.

8.4 The Authority shall be permitted to use and disclose the Supplier's Provisional Supplier Personnel List, the Supplier's Final Supplier Personnel List and the Staffing Information for informing any tenderer or other prospective Replacement Supplier for any services that are substantially the same type of services as (or any part of) the Services.

8.5 The Supplier warrants to the Authority and the Replacement Supplier that the Supplier's Provisional Supplier Personnel List, the Supplier's Final Supplier Personnel List and the Staffing Information ("**TUPE Information**") will be true and accurate in all material respects and that no persons are employed or engaged in the provision of the Services other than those included on the Supplier's Final Supplier Personnel List.

8.6 The Supplier shall and shall procure that any Subcontractor shall ensure at all times that it has the right to provide the TUPE Information under Data Protection Legislation.

8.7 Any change to the TUPE Information which would increase the total employment costs of the staff in the 12 months prior to the Expiry Date and/or the period following the date of service of a Termination Notice by either Party, shall not (so far as reasonably practicable) take place without the Authority's prior written consent, unless such changes are required by law. The Supplier shall and shall procure that any

Subcontractor shall supply to the Authority full particulars of such proposed changes and the Authority shall be afforded reasonable time to consider them.

8.8 In the 12 months prior to the Expiry Date and the period following the date of service of a Termination Notice by either Party, the Supplier shall not and shall procure that any Subcontractor shall not materially increase or decrease the total number of staff listed on the Supplier's Provisional Supplier Personnel List, their remuneration, or make any other change in the terms and conditions of those employees without the Authority's prior written consent.

8.9 The Supplier shall be responsible for all remuneration, benefits, entitlements and outgoings in respect of the Supplier's Personnel, including without limitation, all wages, holiday pay, bonuses, commissions, payments of PAYE, National Insurance, pension contributions and otherwise, up to the Relevant Transfer Date.

8.10 The Supplier shall indemnify and keep indemnified in full the Authority and at the Authority's request each and every Replacement Supplier against all Employee Liabilities relating to:

8.10.1 any person who is or has been employed or engaged by the Supplier or any Subcontractor in connection with the provision of any of the Services; or

8.10.2 any trade union or staff association or employee representative,

arising from or connected with any failure by the Supplier and/or any Subcontractor to comply with any legal obligation, and whether any such claim arises or has its origin before or after the Relevant Transfer Date.

8.11 The Authority will and/or shall ensure that any Replacement Supplier will indemnify and keep indemnified in full the Supplier against any liability to the extent only arising from any failure by the Authority and/or any Replacement Supplier to comply with their obligations under TUPE.

8.12 The parties shall co-operate to ensure that any requirement to inform and consult with the employees and or employee representatives in relation to any Relevant Transfer as a consequence of a Subsequent Transfer will be fulfilled.

8.13 The parties agree that the Contracts (Rights of Third Parties) Act 1999 shall apply in respect of paragraph 8.2 to paragraph 8.10 to the extent necessary to ensure that any Replacement Supplier shall have the right to enforce the obligations owed to, and indemnities given to, the Replacement Supplier by the Supplier or the Authority in its own right under the Contracts (Rights of Third Parties) Act 1999.

8.14 Despite paragraph 8.13, it is expressly agreed that the parties may by agreement rescind or vary any terms of this Contract without the consent of any other person who has the right to enforce its terms or the term in question despite that such rescission or variation may extinguish or alter that person's entitlement under that right.

Schedule 12: Annex 1 – Exit Plan

The content for this Annex is contained in a separate file at:

S12_A1_GEN2W1_DSS_Q10.4_Exit_Plan

S12_A1_GEN2W1_DSS_Q10.4_Entry_Plan

Schedule 12: Annex 1 – Exit Plan

Exit Plan

S12 _A1_GEN2W1_DSS_Q10.4_Exit_Plan

Schedule 12 Annex 1

Entry Plan

S12_A1_GEN2W1_DSS_Q10.4_Entry_Plan

Schedule 13

Form of Guarantee

Not Used

Schedule 14

Form of Assignment and Licence

DATED

THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION

and

[*Supplier*]

INTELLECTUAL PROPERTY ASSIGNMENT AND LICENCE IN RELATION TO THE [xxx] T LEVEL TECHNICAL QUALIFICATION

[***DN: The highlighted details above are to be completed at the Contract award stage***]

THIS ASSIGNMENT AND LICENCE is made on

BETWEEN:

(1) **THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION** of Sanctuary Buildings, 20 Great Smith Street, London SW1P 3BT ("**Authority**"); and

(2) **[*DN: Insert Supplier name and details at Contract award stage*]** ("**Supplier**"),

each a "**Party**" and together the "**Parties**".

BACKGROUND TO THIS ASSIGNMENT AND LICENCE

(A) The Authority and the Supplier have entered into a contract on the date of this Assignment and Licence for the design, development and delivery of the technical education qualification element ("**TQ**") for the [*DN: Relevant pathway to be inserted at Contract award stage*] T Level ("the **TQ Agreement**").

(B) The Supplier has agreed to assign certain intellectual property rights to the Authority, and to licence certain intellectual property rights to the Authority in connection with the TQ. The Authority has agreed to grant a licence back to the Supplier in relation to certain assigned intellectual property rights.

(C) This Assignment and Licence, together with the TQ Agreement sets out the agreed terms of such assignment and licences.

1 Assignment and Licence start, formation and interpretation

1.1 This Assignment and Licence is legally binding from the Effective Date until it ends in accordance with its terms.

1.2 In this Assignment and Licence, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this clause 1 or, where no definition is given in this clause 1, Schedule 1 to the TQ Agreement.

1.3 If a capitalised expression does not have an interpretation in this clause 1 or Schedule 1 to the TQ Agreement, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.4 In this Assignment and Licence, unless the context otherwise requires:

1.4.1 the singular includes the plural and vice versa;

1.4.2 reference to a gender includes the other gender and the neuter;

1.4.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.4.4 references to a legal entity (other than the Supplier) shall include unless otherwise expressly stated any statutory successor to such entity and/or the relevant functions of such entity, and references to the Department shall include, where relevant, the ESFA;

1.4.5 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.4.6 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.4.7 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.4.8 references to "**clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of this Assignment and Licence and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.4.9 references to "**paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and

1.4.10 the headings in this Assignment and Licence are for ease of reference only and shall not affect the interpretation or construction of this Assignment and Licence.

1.5 In this Assignment and Licence, unless the context otherwise requires, the following words shall have the following meanings:

"**Ancillary Materials**" means all information and materials (other than Key Materials) to which the Authority and/or a Future Supplier would require access for the Portability Purposes, and any other materials which would be required on or to facilitate succession to a Future Supplier in a seamless manner in relation to the TQ offered or Operated by the Supplier.

Ancillary Materials shall include, without limitation:

(a) Student results including grades;

(b) statistical analysis for grading (excludes the systems supporting the analysis);

(c) lists of Providers;

(d) marked Student evidence (with moderation outcomes);

(e) documentation which provides an overview or analysis of Student performance (including chief examiner and chief moderator reports), which include but are not limited to, examples of student responses to assessment questions and/or tasks as well as narrative explaining why students did well/ less well on individual items/ components/ subcomponents);

(f) data on Student credits;

(g) data on Student appeals;

(h) data on special considerations for Students;

(i) the Assessment Strategy;

(j) Student registrations;

(k) draft materials in preparation for forthcoming assessments;

(l) the Key Dates Schedule (in respect of forthcoming assessments);

(m) lists, with contact details, of people contracted by the Supplier to perform or oversee activities which are necessary for the conduct and quality assurance of assessments for the TQ;

(n) materials from completed assessments, such as completed Students' examination answer booklets; and

(o) TQ Live Assessment Materials

"**Approval**" has the same meaning as in the TQ Agreement;

"**Assigned Rights**" means the Intellectual Property Rights in the Key Materials;

"**Authority Authorised Representative**" has the same meaning as in the TQ Agreement;

"**Background IPR**" means any IPR owned by a Party prior to the Effective Date or created or developed by a Party otherwise than in the provision of the Services or under or in connection with the TQ Agreement, but does not include IPR in Key Materials;

"**Beneficiary**" means a Party having (or claiming to have) the benefit of an indemnity under this Assignment and Licence;

"**Claim**" means any claim for which it appears that a Beneficiary is, or may become, entitled to indemnification under this Assignment and Licence;

"**Continuing Activities**" means activities of the Supplier under the TQ Agreement which continue following the end of the second Academic Year for the final Exclusive Cohort (each as defined in the TQ Agreement) in relation to the TQ as offered by the Supplier, such as retakes, appeals, and any ongoing records management contracted to the Supplier;

"**Default**" means any breach of the obligations of the Supplier (including abandonment of the Assignment and Licence in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its

Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of this Assignment and Licence and in respect of which the Supplier is liable to the Authority;

"**Deliverables**" means all information and data the Supplier creates, identifies for use, or uses as part of or for the Operation of the TQ, including Products and Management Information;

"**Dispute**" means any claim, dispute or difference which arises out of or in connection with this Assignment and Licence or in connection with the negotiation, existence, legal validity, enforceability or termination of this Assignment and Licence, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;

"**Effective Date**" means the date on which the last Party to sign has signed this Assignment and Licence;

"**Final Approval Milestone**" has the meaning given in the TQ Agreement;

"**Future Supplier**" means any Awarding Organisation appointed, at any point in the future and including any Replacement Supplier, to operate one or more T Level technical education qualifications by or at the direction of the Authority from time to time, and where the Authority is operating a T Level technical education qualification, shall also include the Authority;

"**Indemnifier**" means a Party from whom an indemnity is sought under this Assignment and Licence;

"**Insolvency Event**" means:

(a) in respect of a company:

(i) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or

(ii) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or

(iii) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or

(iv) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or

(v) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or

(vi) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or

(vii) being a "**small company**" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

(b) where the person is an individual or partnership, any event analogous to those listed in limbs (a) (i) to (vii) (inclusive) occurs in relation to that individual or partnership; or

(c) any event analogous to those listed in limbs (a) (i) to (vii) (inclusive) occurs under the law of any other jurisdiction;

"**Intellectual Property Rights**" or "**IPR**" means:

(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography

rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

"**IPR Claim**" means any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR used to provide the Services and/or supply the Products or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority in the fulfilment of its obligations under the TQ Agreement or this Assignment and Licence;

"**Key Materials**" means materials the IPR in which the Authority reasonably requires ownership of for the Portability Purposes. Examples of where the Authority may reasonably require ownership include because the Authority or a Future Supplier (or, where relevant, a potential Future Supplier) may need to copy or otherwise reproduce such materials (in whole or in part), to supply or communicate the same, or to be able control the use (in whole or in part) of such materials by third parties, or to authorise others to do so.

Key Materials shall include:

(a) specifications of content for each TQ including core and all specialist components;

(b) assessment guidelines (for Providers);

(c) quality assurance requirements (for Providers);

(d) specimen assessment materials;

(e) standards exemplification materials;

(f) supplementary specimen assessment materials

(g) employer set project guide exemplar responses

(h) employer set project grade exemplar responses

(i) updates or redevelopments of specifications of content;

(j) updates and redevelopments of any Key Materials; and

(k) any materials equivalent to the above to which a Skilled Future Supplier would reasonably require access for the Portability Purposes.

Key Materials shall not include:

(1) Support Materials, insofar as they are not part of any of the expressly included items listed above;

(2) question banks insofar as they are not part of any of the included items listed above and are not developed for the TQ; and

(3) any systems and platforms used to support the delivery of the TQ, provided that the relevant TQ content or data held in or processed by such systems and/or platforms can be extracted without requiring further processing post-extraction (and the Supplier can demonstrate that they can be so extracted) to enable use of the relevant content and/or data by a Skilled Future Supplier in conjunction with a non-proprietary or generally commercially available system or platform;

"**Know-How**" means all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Services;

"**Law**" means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;

"**Losses**" means all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;

"**New IPR**" means :

(a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of the TQ Agreement and updates and amendments of these items including (but not limited to) database schema; and/or

(b) IPR in or arising as a result of the performance of the Supplier's obligations under the TQ Agreement and all updates and amendments to the same,

but shall not include any IPR owned by the Supplier prior to the Effective Date;

"**Operate**" in relation to a qualification means to provide the Services or a material part of the Services, or services replacing the Services or a material part of the Services, or of an equivalent character to the Services or a material part of the Services in relation to any other qualification (whether a T Level technical education qualification or not); and "**Operation**" and other cognate terms shall have a corresponding meaning;

"**Party**" means the Authority or the Supplier and "**Parties**" means both of them where the context permits;

"**Product**" has the meaning given in the TQ Agreement;

"**Provider**" means an organisation that has a grant agreement and/or a contract in place with the ESFA to provide qualifications to Students;

"**Replacement Services**" means any services which are substantially similar to any of the Services (including the supply of any Products) and which the Authority receives in substitution for any of the Services, whether those services are provided by the Authority internally and/or by any third party;

"**Replacement Supplier**" has the meaning given in the TQ Agreement;

"**Required Insurances**" has the meaning given in the TQ Agreement;

"**Services**" means the services as described in Schedule 2 to the TQ Agreement (*Service Requirements*) including any Additional Services as defined in the TQ Agreement;

"**Termination Notice**" means a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Assignment and Licence on a specified date and setting out the grounds for termination;

"**Third Party IPR**" means Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Services and/or supplying the Products;

"**TQ Agreement**" has the meaning given in recital A (above);

"**Transparent**" means that students and employers will regard the TQ delivered by a Future Supplier as materially the same as the TQ delivered and operated by the (existing) Supplier;

"**Working Day**" means any day other than a Saturday or Sunday or public holiday in England and Wales.

2 Assignment

2.1 Pursuant to and for the consideration set out in the TQ Agreement, the Supplier assigns to the Authority, absolutely with full title guarantee all its right, title and interest in and to all of the Intellectual Property Rights in the Key Materials (which, for the avoidance of doubt, includes the Guide Standard Exemplification Materials) including the right to bring, make, oppose, defend, appeal proceedings, claims or actions and obtain relief (and to retain any damages recovered) in respect of any infringement, or any other cause of action arising from ownership, of any of the Assigned Rights on or after the date of this Assignment and Licence. Such assignment shall take place on the earlier of:

2.1.1 the creation of any relevant materials known to be Key Materials;

2.1.2 the identification by the Supplier of the use of the relevant materials as part of the TQ; and

2.1.3 delivery of the relevant Key Materials to the Authority, or Operation of the TQ by the Supplier.

2.2 With the exception of Guide Standard Exemplification Materials, all Key Materials are relevant course documents for the purposes of section A2D3(4) of the Apprenticeships, Skills, Children and Learning Act 2009, and on approval of the TQ at the Final Approval Milestone and on any subsequent Approval, to the extent that any copyright or any rights in copyright forming part of the Assigned Rights have not then been assigned to and vested absolutely in the Authority, they shall be transferred to the Authority by operation of statute in accordance with section A2IA of the Apprenticeships, Skills, Children and Learning Act 2009. Intellectual Property Rights in the Guide Standard Exemplification Materials is assigned to the Authority by virtue of 2.1 above.

3 Licences to the Authority

3.1 The Supplier hereby grants to the Authority (and the Authority shall have, in addition to any retained rights under clause 13.8 of the TQ Agreement) a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, exploit and sub-license the IPR in the Ancillary Materials and the Supplier's Background IPR and, in respect of any IPR in Key Materials, in each case to the extent that the same are not at the relevant time vested absolutely in the Authority, as necessary to enable the Authority (and its sub-licensees) to:

3.1.1 use the Key Materials and Ancillary Materials in its administration, approval and oversight of the TQ and other T Level technical education qualifications and to make the same available to others (such as Ofqual) to do the same; and

3.1.2 to use the Key Materials and the Ancillary Materials, and for any Future Supplier or potential Future Supplier to use the Key Materials and the Ancillary Materials:

(i) for competing or tendering for the delivery and Operation of the TQ and/or any Replacement TQ, during any Transition Period and following expiry or termination of the TQ Agreement; and

(ii) to deliver and Operate the TQ and any Replacement TQ, during any Transition Period and following expiry or termination of the TQ Agreement; and

3.1.3 otherwise to receive and use the Services and the Deliverables and allow any Future Supplier to use the Deliverables; and

3.1.4 to sub-license others to exercise the rights set out in this clause 3.1.

3.2 The Authority agrees that it shall use any Ancillary Materials which fall solely within element (l) of the definition of Ancillary Materials (being "*lists, with contact details, of people contracted by the Supplier to perform or oversee activities which are necessary for the conduct and quality assurance of assessments for the TQ*") only for the purposes of planning for or executing an Emergency Exit.

4 Licence to the Supplier

4.1 The Authority hereby grants to the Supplier, in respect of the Assigned Rights, a worldwide, royalty free, perpetual and irrevocable non-exclusive licence, with the right to sublicense, to use and exploit the IPR in the Key Materials during and after the Term, but not, save as provided in the TQ Agreement, to use the same as part of a T Level, such licence being subject to clauses 13.13 and 13.14 of the TQ Agreement (which for these purposes shall survive any termination or expiry of the TQ Agreement).

5 Warranties and representations

5.1 The Supplier warrants and represents (on the Effective Date and on any relevant assignment or grant of licence taking effect) that:

5.1.1 it is or will be the sole legal and beneficial owner of, and that it owns all the rights and interests in the Assigned Rights no later than the time for assignment specified in clause 2.1 or when they are assigned in accordance with clause 13.2.1 of the TQ Agreement, save for Assigned Rights other than New IPR, in respect of which it has previously notified the

Authority and the Authority has agreed in writing that this warranty shall not apply;

5.1.2 where it is not the sole legal and beneficial owner of the Assigned Rights, including the Assigned Rights which are to be used or embodied in any Key Materials, it has established that all owners of such rights consent to their assignment and transfer absolutely to the Authority;

5.1.3 it has all the necessary right and title to grant all the licences granted to the Authority under this Assignment and Licence and the TQ Agreement;

5.1.4 it has not licensed or assigned any of the Assigned Rights other than pursuant to this Assignment and Licence or the TQ Agreement;

5.1.5 the Assigned Rights are free from any security interest, option, mortgage, charge or lien;

5.1.6 it is unaware of any infringement or likely infringement of any of the Assigned Rights;

5.1.7 as far as it is aware, all the Assigned Rights are valid and subsisting and there are and have been no claims, challenges, disputes or proceedings, pending or threatened, in relation to the ownership, validity or use of any of the Assigned Rights;

5.1.8 the use of the Key Materials and Ancillary Materials, and exploitation of the Assigned Rights by the Supplier in the provision of the Services and Deliverables or by the Authority in receiving and using the Services and Deliverables or procuring any Replacement Services or by any Future Supplier in Operating any Replacement Services, will not infringe the rights of any third party; and

5.1.9 the Key Materials are its original work and have not been copied wholly or substantially from any other source.

6 Indemnity

6.1 Subject to clause 19, if there is an IPR Claim, the Supplier indemnifies the Authority against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

6.2 If an IPR Claim is made or anticipated, the Supplier must at its own expense and the Authority's sole option, either:

6.2.1 obtain for the Authority the rights in clause 2.1 and 3.1 without infringing any Third Party IPR; or

6.2.2 replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.

7 Moral rights

7.1 The Supplier shall procure written absolute waivers from all authors of the Key Materials and Ancillary Materials in relation to all their moral rights arising under the Copyright, Designs and Patents Act 1988 in relation to the Key Materials and Ancillary Materials and, as far as is legally possible, any broadly equivalent rights such authors may have in any territory of the world.

8 Ending or extending the Assignment and Licence

8.1 This Assignment and Licence ends if terminated by the Authority for any reason set out in this Assignment and Licence.

8.2 If any of the following events happen, the Authority has the right to immediately terminate this Assignment and Licence or any of the licences granted under this Assignment and Licence by issuing a Termination Notice to the Supplier (in the latter case specifying the relevant licences):

8.2.1 a Default incapable of remedy;

8.2.2 a Default capable of remedy that is not corrected within 30 days; and

8.2.3 anything occurs which entitles the Authority to terminate the TQ Agreement.

9 Claims against third parties

9.1 The Supplier may take any action it considers appropriate or necessary, subject to the Authority's prior written consent, not to be unreasonably withheld or delayed, if there is a breach, other than in connection with the TQ, by a third party of the Authority's rights in any IPR licensed to the Supplier under clause 4, and the Authority agrees to provide all such assistance as the Supplier may reasonably require (subject to meeting the Authority's reasonably agreed costs and expenses and the Supplier hereby indemnifying the Authority in respect of any loss, damage or liability the Authority incurs by reason of any such action).

10 Further assurance

10.1 At the Authority's expense the Supplier shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this Assignment and Licence and the TQ Agreement, including:

10.1.1 registration of the Authority as applicant or (as applicable) proprietor of the Assigned Rights; and

10.1.2 assisting the Authority in obtaining, defending and enforcing the Assigned Rights, and assisting with any other proceedings which may be brought by or against the Authority against or by any third party relating to the Assigned Rights.

10.2 The Supplier appoints the Authority to be its attorney in its name and on its behalf to execute documents, use the Supplier's name and do all things which are necessary or desirable for the Authority to obtain for itself or its nominee the full benefit of this Assignment and Licence.

10.3 This power of attorney is irrevocable and is given by way of security to secure the performance of the Supplier's obligations under this Assignment and Licence and the proprietary interest of the Authority in the Assigned Rights and so long as such obligations of the Supplier remain undischarged, or the Authority has such interest, the power may not be revoked by the Supplier, save with the consent of the Authority.

10.4 Without prejudice to clause 10.2, the Authority may, in any way it thinks fit and in the name and on behalf of the Supplier:

10.4.1 take any action that this Assignment and Licence requires the Supplier to take;

10.4.2 exercise any rights which this Assignment and Licence gives to the Supplier; and

10.4.3 appoint one or more persons to act as substitute attorney(s) for the Supplier and to exercise such of the powers conferred by this power of attorney as the Authority thinks fit and revoke such appointment.

10.5 The Supplier undertakes to ratify and confirm everything that the Authority and any substitute attorney does or arranges or purports to do or arrange in good faith in exercise of any power granted under this clause 10.

11 How much each Party can be held responsible for

11.1 Each Party's total aggregate liability under this Assignment and Licence (whether in tort, contract or otherwise) for each claim or series of connected claims is no more than £1 million.

11.2 No Party is liable to the other for:

11.2.1 any indirect Losses; or

11.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

11.3 The limitation of liability set out in clause 11.1 does not apply to either Party in relation to the following:

11.3.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or subcontractors;

11.3.2 bribery or fraud or fraudulent misrepresentation by it or its employees; or

11.3.3 any liability that cannot be excluded or permitted by Law.

11.4 Each Party must use all reasonable endeavours to mitigate any Losses which it suffers under or in connection with this Assignment and Licence, including where any such Losses are covered by an indemnity.

11.5 When calculating the Supplier's liability under clause 11.1, Losses covered by Required Insurances will not be taken into consideration.

12 Invalid parts of this Assignment and Licence

12.1 If any part of this Assignment and Licence is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be removed from this Assignment and Licence as much as required and rendered ineffective as far as possible without affecting the rest of the Assignment and Licence, or whether it is valid or enforceable.

13 No other terms apply

13.1 Except as otherwise expressly provided in this Assignment and Licence or in the TQ Agreement, the provisions incorporated into this Assignment and Licence are the entire agreement between the Parties. The Assignment and Licence replaces all previous statements and agreements whether written or oral. No other provisions apply.

13.2 Variation of this Assignment and Licence is only effective if agreed in writing and signed by both Parties.

14 Other people's rights in this Assignment and Licence

14.1 No third parties may use the Contracts (Rights of Third Parties) Act ("**CRTPA**") to enforce any term of this Assignment and Licence unless stated (referring to CRTPA) in this Assignment and Licence. This does not affect third party rights and remedies that exist independently from CRTPA.

15 Relationships created by this Assignment and Licence

15.1 This Assignment and Licence does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

16 Giving up contract rights

16.1 A partial or full waiver or relaxation of the terms of this Assignment and Licence is only valid if it is stated to be a waiver in writing to the other Party.

17 Transferring responsibilities

17.1 The Supplier must not assign this Assignment and Licence without Approval.

17.2 The Authority can assign, novate or transfer this Assignment and Licence or any part of it to any Crown Body, public or private sector body which performs the functions of the Authority.

17.3 The Supplier must enter into a novation agreement in the form that the Authority specifies in order to use its rights under clause 17.2.

17.4 The Supplier can terminate this Assignment and Licence if it is novated under clause 17.2 to a private sector body that is experiencing an Insolvency Event.

18 How to communicate about this Assignment and Licence

18.1 All notices under this Assignment and Licence must be in writing and are considered effective on the Working Day of delivery as long as delivered before 5:00 pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

18.2 Notices to the Authority must be sent to the Authority Authorised Representative's address and email address, and all notices must be copied to the Authority's Head of Commercial Delivery Management (xxx@education.gov.uk) and the Authority's Head of Legal (xxx@education.gov.uk) .

18.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

19 Dealing with claims

19.1 If a Beneficiary is notified or otherwise becomes aware of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days after such notification or date of first awareness.

19.2 At the Indemnifier's cost the Beneficiary must both:

19.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and

19.2.2 give the Indemnifier reasonable assistance with the Claim if requested.

19.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

19.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary's reputation.

19.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

19.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

19.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

19.7.1 the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or

19.7.2 the amount the Indemnifier paid the Beneficiary for the Claim.

20 Resolving disputes

20.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

20.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or

continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using clauses 20.3 to 20.5.

20.3 Unless the Authority refers the Dispute to arbitration using clause 20.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

20.3.1 determine the Dispute;

20.3.2 grant interim remedies, or any other provisional or protective relief.

20.4 The Supplier agrees that the Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

20.5 The Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 20.4, unless the Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 20.4.

20.6 The Supplier cannot suspend the performance of this Assignment and Licence during any Dispute.

21 Which law applies

21.1 This Assignment and Licence and any issues arising out of, or connected to it, are governed by English law.

ANNEX

IPR Assurance Certificate

This certificate is given pursuant to clause 13.9 of the agreement ("**Contract**") between the Institute for Apprenticeships and Technical Education ("**Authority**") and the supplier named below ("**Supplier**"), and the Intellectual Property Assignment and Licence between the Authority and the Supplier (which also forms Schedule 14 of the Contract) ("**Assignment and Licence**").

Guidance:

When to complete this certificate: This certificate should be completed in respect of each Deliverable (as defined in the Contract) which is made available to the Authority under the Contract, and a completed certificate should be supplied to the Authority with that Deliverable. This includes updates to existing Deliverables.

Purpose of this certificate: This certificate is intended to confirm that the specific Deliverable fully complies with the intellectual property provisions of the Contract. A copy of the certificate will be retained by the Authority as evidence of the intellectual property position.

Supplier Declaration:

We (being the Supplier named below) confirm that the Deliverable(s) supplied together with (or shortly before or after) this certificate, all elements of which are listed in either Table 1 or Table 2 below[1], comply with the intellectual property provisions in the Contract, in particular the applicable warranties set out in clause 5 of the Assignment and Licence.

We confirm that the Deliverable(s) either:
(i) contain no third party intellectual property rights, or
(ii) contain third party intellectual property rights and we have obtained the consent of the applicable third party:

- in the case of Key Materials, to their assignment and transfer to the Authority; and/or
- in the case of Ancillary Materials, to their licence to the Authority,

in each case on the terms and conditions of the Contract and Assignment and Licence.

We confirm that this certificate overrides any statement or copyright notice forming part of the Deliverable(s) which is in any way inconsistent with this certificate. We agree that this certificate does not detract in any way from the rights granted to the Authority in the Contract.

Key Materials

We confirm that the Deliverable(s) set out in Table 1 below, or the elements of the Deliverable(s) set out in Table 1 below, are Key Materials, as defined in the Contract:

[1] If, by exception, the Supplier asserts that the Deliverable includes elements which are neither Key Materials nor Ancillary Materials, this should be notified in writing to the Authority prior to the relevant Deliverable being made available to the Authority.

Table 1

Deliverable	Key Materials
[Set out title / description of the Deliverable]	Set out elements which are Key Materials, or confirm "entire Deliverable"
[insert additional rows if required]	

All intellectual property rights in the Deliverable(s), or elements of the Deliverable(s) listed above in Table 1 as Key Materials, have vested or hereby vest in the Authority pursuant to the Assignment and Licence.

Ancillary Materials

We confirm that the Deliverable(s) set out in Table 2 below, or the elements of the Deliverable set out in Table 2 below are Ancillary Materials, as defined in the Contract:

Table 2

Deliverable	Ancillary Materials
[Set out title / description of the Deliverable]	Set out elements which are Ancillary Materials, or confirm "entire Deliverable"
[insert additional rows if required]	

All intellectual property rights in the Deliverable(s), or elements of the Deliverable(s) listed above in Table 2 as Ancillary Materials, are licensed to the Authority on the terms and conditions of and pursuant to the Assignment and Licence.

Signed for and on behalf of the Supplier:

Name

Position

Date

Signed by

[*Supplier*]

Director: ……..[*Insert/print name*]

Signature: ……...

Signed by

THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION

Director: ……..[Insert/print name]

Signature: ……...

Schedule 15

Monitoring of Performance

1 Self monitoring

1.1 The Supplier shall monitor its performance of the Services (other than the Initial Development Services) and (where applicable) the supply of the Products against each KPI (in the manner set out in paragraph 1.2) and shall deliver to the Authority Authorised Representative the Operational Delivery Report in accordance with paragraph 3 (*Operational Delivery Report and Performance Review Meetings*).

1.2 The Supplier shall, in respect of each KPI, apply the applicable Performance Monitoring Methodology to such KPI to assess the Supplier's performance of such relevant KPI during the relevant Performance Monitoring Period.

2 What happens if you don't meet the Service Levels

2.1 The Supplier shall at all times provide the Services and (where applicable) supply the Products to meet or exceed the Target Service Level for each KPI.

2.2 If, in any Contract Month in which a Performance Monitoring Period for a KPI ends, the Supplier fails to achieve the Target Service Level for that KPI ("**Service Failure**"), the Supplier shall submit to the Authority (as part of the Operational Delivery Report for that Contract Month) for Approval an improvement plan ("**KPI Improvement Plan**") setting out:

2.2.1 the reasons for such Service Failure; and

2.2.2 what steps the Supplier proposes to take to:

(i) mitigate the impact of the Service Failure;

(ii) rectify the event, matter or circumstance giving rise to the Service Failure (including details of the proposed timings for such rectification); and

(iii) prevent the Service Failure from recurring.

2.3 The Authority shall (as soon as reasonably practicable following receipt of the KPI Improvement Plan) either:

2.3.1 confirm to the Supplier that the KPI Improvement Plan is Approved and following receipt of such Approval the Supplier shall:

(i) carry out and complete all of the actions in accordance with the approved KPI Improvement Plan; and

(ii) report on its progress against such KPI Improvement Plan in each and every Performance Review Meeting which occurs whilst the Supplier is (or should be, if it was complying with its obligations under this Contract) carrying out and completing the actions in accordance with the KPI Improvement Plan; or

2.3.2 confirm to the Supplier that the Authority is not satisfied with the KPI Improvement Plan and/or that the steps proposed by the Supplier in the KPI Improvement Plan will address the matters referred to in paragraph 2.2.1, in which case the provisions of clause 14.2 (*What may happen if there are issues with your provision of the Services*) shall apply.

2.4 Where:

2.4.1 the Supplier fails to provide a KPI Improvement Plan in accordance with paragraph 2.2; or

2.4.2 following Approval by the Authority of the KPI Improvement Plan in accordance with paragraph 2.3, the Supplier fails to carry out and/or complete the actions in accordance with the KPI Improvement Plan (as Approved),

then such failure shall be deemed to be a Critical Service Failure.

3 Operational Delivery Report and Performance Review Meetings

3.1 Within 5 Working Days after the end of each Contract Month, the Supplier shall deliver to the Authority Authorised Representative the Operational Delivery Report in respect of the performance by the Supplier of the Services (and (where applicable) the supply

of the Products) during the Contract Month just ended together with updated versions (meeting, where applicable, all of the requirements of the relevant Product Description) of the following:

3.1.1 the Implementation and Delivery Plan;

3.1.2 the Resource Plan;

3.1.3 the Risk Register;

3.1.4 the Issues Log;

3.1.5 the Assessment Strategy; and

3.1.6 any draft version of the Key Dates Schedule that the Supplier intends shall (if Approved) become the Key Dates Schedule for the purposes of this Contract from time to time.

3.2 Within 5 Working Days of receipt by the Authority Authorised Representative of the Operational Delivery Report for the relevant Contract Month, the Parties shall attend a meeting to discuss the content of the relevant Operational Delivery Report (the "**Performance Review Meeting**") at such location and time (within normal business hours) as the Authority shall reasonably require and such Performance Review Meeting shall:

3.2.1 be attended by the Authority Authorised Representative and the Supplier Authorised Representative and/or such other senior representatives of either Party as the Authority Authorised Representative and/or the Supplier Authorised Representative shall reasonably require (having regard to the matters to be discussed at the relevant Performance Review Meeting); and

3.2.2 be fully minuted by the Supplier and the minutes shall be circulated by the Supplier to all attendees at the relevant Performance Review Meeting (and any other recipients agreed at the relevant meeting) as soon as reasonably practicable following the relevant Performance Review Meeting.

3.3 The minutes of the preceding Contract Month's Performance Review Meeting will be agreed and signed by both the Authority Authorised Representative and the Supplier Authorised Representative at or prior to the following Performance Review Meeting.

3.4 Without prejudice to clause 9 (*Record keeping, monitoring and reporting*), the Supplier shall provide to the Authority such additional information and/or documentation as the Authority may reasonably require in order to verify the Supplier's compliance with its obligations under this Contract, including to verify:

3.4.1 whether a Service Failure has occurred; and/or

3.4.2 the level of the performance by the Supplier of the whole or any part of the Services and (where applicable) the supply of the Products,

and the Supplier shall provide such information and/or documentation within such time period as the Authority shall reasonably specify at the time of making the request for such information and/or documentation.

Schedule 15: Annex 1 – Key Performance Indicators

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
1. The Supplier has in place clear and TQ specific arrangements to approve Eligible Providers and monitor Approved Providers and (i) completes the relevant processes for approval quickly upon application and (ii) carries out the required monitoring	TQ Provider approval and monitoring services – paragraph 3	(i) 100% of applications from Eligible Providers decided within 30 Working Days of receipt of application; and (ii) Supplier has carried out the required monitoring in accordance with the Implementation and Delivery Plan and/or the	Each Contract Month following IfATE Approval	Management Information in relation to: (i) Eligible Providers that have applied for approval and in respect of which a decision has been made; and (ii) details of monitoring undertaken.	Performance measurement will include Eligible Providers new to the Supplier as well as the Supplier's existing Eligible Providers who have applied to have their approval extended to include the TQ.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
		Assessment Strategy.			
2. Supplier has ensured that Approved Providers are clear about what they are expected to teach and to what standard of attainment, and about how Students will be assessed	Initial TQ deliverables and development services – paragraph 2 TQ Provider support services – paragraph 4 TQ live assessment design and delivery – paragraph 6	80% of Approved Providers that have responded to the survey, rating at least 4 on a 1-5 scale. The target performance scale will use 2 positive, 2 negative and 1 neutral response. (For example (noting that the exact wording of the descriptors may vary)	During the Summer Term each Academic Year from September 2025	The Authority shall undertake or commission a survey of Approved Providers delivering the TQ	Online questionnaire to Approved Providers delivering the TQ in the relevant Academic Year. This survey should achieve a minimum response rate of 20% of those surveyed to be valid

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
		where 5 = very clear 4 = mostly clear 3 = moderately clear 2 = mostly unclear 1 = not clear at all)			
3. Queries from Eligible Providers and Approved Providers (other than those related to KPI 4 and KPI 11) are satisfactorily resolved in accordance with the Target Service Level	Initial TQ deliverables and development services – paragraph 2 TQ Provider approval and monitoring services – paragraph 3 TQ Provider support services – paragraph 4 Student registration and student entry – paragraph 5	Queries raised by letter and other forms of electronic correspondence: 90% resolved within 10 Working Days; remaining 10% resolved within 15 Working Days; and Queries raised through telephone	Each Contract Month from the Effective Date	Management Information based on data and information collected from the Supplier's customer management systems referred to in Service Requirement 5 in Part 2 of the Service Requirements. This must include relevant information that closed queries have been satisfactorily resolved.	The required resolution time commences on and from the Working Day on which the relevant query is received by the Supplier Percentage of queries that are resolved in accordance with the applicable Target Service Level

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
	TQ live assessment design and delivery – paragraph 6 TQ Post-Results Services – paragraph 9	calls: 90% resolved within 2 Working Days; remaining 10% resolved within 10 Working Days			
4. Formal complaints made about the Services are satisfactorily resolved (i) in accordance with the timescales set out in the Implementation and Delivery Plan[2] or (ii) where complaints are received solely by the Department, ESFA or the Authority, within the timescales reasonably required by the Department, ESFA	Initial TQ deliverables and development services – paragraph 2 TQ Provider approval and monitoring services – paragraph 3 TQ Provider support services – paragraph 4 Student registration and student entry – paragraph 5	100% of formal complaints are resolved within: (i) the relevant timescales detailed in the Implementation and Delivery Plan; or (ii) the timescales specified by the Department, ESFA or the Authority,	Each Contract Month from the Effective Date	Management Information based on data and information collected from the Supplier's customer management systems referred to in Service Requirement 5 in Part 2 of the Service Requirements. This must include relevant information that complaints have been satisfactorily resolved.	The required resolution time commences on and from the Working Day on which the relevant complaint is received by the Supplier. Percentage of complaints that are satisfactorily resolved within the applicable Target Service Level. Any complaints received solely by the Department, ESFA or

[2] The Supplier Response should detail the Supplier's proposals for resolving formal complaints.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
or the Authority at the time of notifying the Supplier of such complaints	TQ live assessment design and delivery – paragraph 6 TQ Post-Results Services – paragraph 9	(as the case may be).			the Authority, in relation to the Services, shall be deemed to have been received by the Supplier on the date on which the Supplier is notified of the complaint by the Department, ESFA or the Authority.
5. Approved Providers are satisfied with the quality of the Provider Services	TQ Provider approval and monitoring services – paragraph 3 TQ Provider support services – paragraph 4 Student registration and student entry – paragraph 5 TQ live assessment design and delivery – paragraph 6	80% of Approved Providers that have responded to the survey, rating at least 4 on a 1-5 scale. The target performance scale will use 2 positive, 2 negative and 1 neutral response. For example (noting that the	During the Summer Term each Academic Year from September 2025	The Authority shall undertake or commission a survey of Approved Providers delivering the TQ	Online questionnaire to Approved Providers delivering the TQ in the relevant Academic Year. This survey should achieve a minimum response rate of 20% of those surveyed to be valid.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
	TQ Post-Results Services – paragraph 9	exact wording of the descriptors may vary) (where 5 = very satisfied 4 = satisfied 3 = neither satisfied nor dissatisfied 2 = dissatisfied 1 = very dissatisfied).			
6.A sufficient number of appropriately qualified and trained Assessors (and Moderators where permitted in accordance with the Approved Assessment Strategy) are available to assess (or Moderate, if	TQ live assessment design and delivery – paragraph 6	100% of appropriately qualified and trained Assessors (and Moderators, if applicable) are available in accordance with the Implementation and Delivery Plan	Each Contract Month from (and including) September 2025	Management Information in relation to Assessor (and Moderator, if applicable) actual recruitment, training, and retention against the details set out in the Implementation and Delivery Plan and	Performance will be measured against the number of Assessors (and Moderators, if applicable) that are envisaged as being trained and available as detailed in the Implementation and Delivery Plan and/or

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
applicable) Student assessment evidence when required in accordance with the Implementation and Delivery and/or the Resource Plan (as the case may be)		and/or the Resource Plan (as the case may be).		Resource Plan (as the case may be).	the Resource Plan (as the case may be).
7. The TQ Live Assessment Materials (as defined in the Service Requirements) are high quality and developed in accordance with the Assessment Strategy	TQ live assessment design and delivery – paragraph 6	Full compliance with parts of both the Assessment Strategy and Implementation Plan that relate to the development of the TQ Live Assessment Materials; and TQ Live Assessment Materials are 100% free of errors that could affect clarity	Each Contract Month from IfATE Approval	Management Information in relation to: (i) progress against and compliance with the relevant part of the Assessment Strategy and Implementation Plan; and (ii) any errors reported in TQ Live Assessment Materials.	Review of Supplier self-reporting Identification of any reported errors in TQ Live Assessment Materials.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
		about requirements for Students.			
8. Student assessment evidence is accurately assessed and processed for grading and awarding in accordance with the relevant parts of the Assessment Strategy and the Implementation and Delivery Plan	TQ live assessment design and delivery – paragraph 6 TQ Grade awarding – paragraph 7	Assessing of Student assessment evidence is conducted in accordance with the relevant parts of the Assessment Strategy; and 100% of Students' assessments are marked and processed in accordance with the relevant parts of the Implementation and Delivery Plan.	Each Contract Month from September 2025 until the end of the Term	Management Information in relation to compliance with the relevant parts of the Assessment Strategy and the relevant parts of the Implementation and Delivery Plan.	Review of Supplier self-reporting.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
9. Grade Standard Exemplification Materials are validated by Employers	TQ live assessment design and delivery – paragraph 6 TQ Grade awarding – paragraph 7	At least 5 Employers in each relevant Occupational Specialist Component.	In October in each Academic Year following the first grade awarding but in any event no later than from October 2027	Evidence of validation from Employers relevant to the Occupational Specialist Components that validate the Grade Standard Exemplification Materials. The Supplier may use its existing network of Employers, but it must ensure a turnover of Employers each Academic Year. Employers may take part in validation activity for up to two consecutive Academic Years, after which they must not take part in validation activity for a period of one Academic Year. Suppliers may then repeat this cycle, ensuring that Employers do not take part in validation activity for	Validation means that Employers relevant to the Occupational Specialist Components judge that the Grade Standard Exemplification Materials are comparable to the Approved Guide Standard Exemplification Materials. Validation also means that Employers relevant to the Occupational Specialist Components judge that the Grade Standard Exemplification Material on the pass boundary is the type of work Employers would expect to see from an employee, who is of Occupational Entry Competence and that the Grade Standard

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
				more than two consecutive Academic Years. For each Occupational Specialist Component, validations are required from at least two new Employers each Academic Year who did not submit evidence of validation in any previous Academic Year.	Exemplification Material on the distinction boundary, is the type of work that exceeds Employer expectations of what they would expect to see from an employee who is of Occupational Entry Competence, as defined within the assessment strategy as distinction. Review by the Authority of the evidence of Validation from Employers.
10. Student assessment results are submitted to the Authority (or its nominee (as applicable)) by the relevant date(s) set	TQ Grade awarding – paragraph 7 TQ Results – paragraph 8	100% of results are submitted to the Authority (or its nominee) by the date(s) set out in the relevant Key Dates Schedule.	Each Contract Month from September 2025 until the end of the Term	Results have been received by the Authority (or its nominee (as applicable)) in the required format.	Receipt of the results by the relevant date(s) in the relevant Key Dates Schedule.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
out in the Key Dates Schedule					
11. Post-Results Services (excluding the issuing of revised assessment results, which is covered by KPI 10) are delivered in accordance with the relevant part of the Assessment Strategy	TQ Post-Results Services – paragraph 9	100% of the Post-Results Services are carried out and completed in accordance with the relevant part of the Assessment Strategy.	Each Contract Month from (and including) September 2025 until the end of the Term	Management Information in relation to compliance with the relevant part of the Assessment Strategy.	Review of self-reporting.
12. Submission to the Authority of: (i) all Management Information in accordance with the requirements of Service Requirement 9	TQ Provider approval and monitoring services – paragraph 3 Student registration and student entry – paragraph 5 Reporting – paragraph 10	100% for timeliness of the submission of all Management Information and all required (including requested) Products and/or	Each Contract Month from the Effective Date	Management Information and updated versions of the Products and/or other documents referred to in column one and/ or Key Materials and Ancillary Materials are received by	Review of self-reporting.

KPI (desired outcome)	Relevant Service Requirements (incl references to the relevant paragraph of Part 1 of the Service Requirements detailing the relevant element of the Services)	Target performance levels	Performance Monitoring Period	Evidence of performance	Measurement methodology
in Part 2 of the Service Requirements; and (ii) updated versions of all required Products in accordance with clause 5.5.1(i) and/or paragraph 3 of Schedule 15 (as the case may be); and (iii) where requested by the Authority, updated versions of all requested Products and/or other documents in accordance with clause 5.5.1(ii).		other documents including Key Materials and Ancillary Materials; and 100% for completeness of all: (i) Management Information; and (ii) required Products (including requested Products and/ or Key Materials and Ancillary materials).		the Authority by the date required by this Contract. Management Information, updated versions of the Products and/or other documents referred to in column one, Key Materials and Ancillary Materials are accurate and complete and cover all relevant information, Data and reports as specified in the Management Information and reporting requirements. Updated versions of the Products referred to in column one, Key Materials and Ancillary Materials include all relevant updates.	

Schedule 16

Logos and Trademarks – T Level Trade Mark Licence

1 Interpretation

The definitions and rules of interpretation in this paragraph apply in this T Level Trade Mark Licence, in addition to the definitions and rules of interpretation in Schedule 1 to this Contract.

1.1 Definitions:

"**Approved Provider**" means an Eligible Provider (as defined in Schedule 1 (*Definitions and Interpretation*) of this Contract) that has been granted Provider Approval (as defined in Schedule 1 (*Definitions and Interpretation*) of this Contract) and in respect of which such Provider Approval has not been revoked pursuant to clause 7.2 of this Contract (*Interaction with Providers*).

"**Brand Licensed Material**" means any instance of a Brand Licensed Product or Service in material form, including as an electronic copy or any other electronic form, and any promotional or marketing material relating to any Brand Licensed Product or Service;

"**Brand Licensed Product or Service**" means any products or services listed as such in Appendix 1 (and "**Brand Licensed Products**" and "**Brand Licensed Services**" means such Products or Services respectively;

"**Mandatory Marked Material**" is material of the type identified in Appendix 1 (and to which the Mark must be applied);

"**Mark**" means the trade mark(s) set out in Appendix 2, including the listed registrations and applications and any registrations which may be granted pursuant to those applications and the related trade marks, devices and get-ups that may be notified in writing by the Authority to the Supplier from time to time;

"**Marked Material**" means any Brand Licensed Material or other material in or on which the Mark is used.

2 Grant

2.1 The Authority hereby grants to the Supplier a non-exclusive licence to use the Mark on or in relation to the Brand Licensed Products or Services provided or supplied in England, including in connection with the promotion, use and supply of the Brand Licensed Products or Services.

2.2 The Supplier may, subject to the prior written approval of the Authority and paragraph 11, sublicense (without the right to further sublicense) each Approved Provider of the TQ to use the Mark on or in relation to the Brand Licensed Products or Services provided or supplied in England, including in connection with the promotion, use and supply of the Brand Licensed Products or Services.

2.3 Any use of the Mark in accordance with paragraph 2.1 or 2.2 shall be strictly in accordance with the T Level Branding Guidelines and, when using the Mark, the Supplier shall fully comply with, the T Level Branding Guidelines.

2.4 Subject to paragraph 2.2, the Supplier shall have no right to sublicense use of the Mark.

3 Application of the Mark

3.1 The Supplier shall use the Mark, in accordance with this Schedule, on all Mandatory Marked Materials.

3.2 Subject to clause 13.10 (*Intellectual Property Rights*) of the Contract and paragraph 3.3 below, apart from the Mark, no other trade mark or logo may be affixed or used in a manner in which it may be seen to be used as a trade mark or designation of origin in relation to any Brand Licensed Products or Services or in or on any Brand Licensed Materials.

3.3 The Supplier may, subject to the prior written agreement of the Authority, authorise each Approved Provider of the TQ sublicensed in accordance with paragraph 2.2 to use the Approved Provider's name, logos, trademarks and/or other signs which refer to the Approved Provider on Brand Licensed Products or Services or Brand Licensed Materials on the same terms as, and subject to compliance with clauses 13.10 and 13.11 (*Intellectual Property Rights*) of the Contract (and clauses 13.10 and 13.11 shall apply *mutatis mutandis* to such Approved Provider).

3.4 The Supplier shall procure that the Mark, when used in or on any Brand Licensed Materials, shall be clearly and reasonably prominently identified as a trade mark of the Authority, in such manner as is set out in the T Level Branding Guidelines, or with any other statement as notified by the Authority to the Supplier.

3.5 The Supplier shall comply strictly with the directions of the Authority regarding the form and manner of the application of the Mark, including the directions contained in the T Level Branding Guidelines.

3.6 The Supplier shall, on written request from the Authority or as otherwise provided in the T Level Branding Guidelines, provide samples of all proposed Marked Materials.

3.7 The Supplier shall not use in its business any other trade mark confusingly similar to the Mark and shall not use the Mark or any word confusingly similar to the Mark as, or as part of, its corporate or trading name.

4 Title, goodwill and registrations

4.1 The Supplier acknowledges that the Authority is the owner of the Mark.

4.2 Any goodwill derived from the use by the Supplier of the Mark shall accrue to the Authority. The Authority may, at any time, call for a document confirming the assignment of that goodwill and the Supplier shall immediately execute it.

4.3 The Supplier shall not do, or omit to do, or permit to be done, any act that will or may weaken, damage or be detrimental to the Mark or the reputation or goodwill associated with the Mark or the Authority, or that may invalidate or jeopardise any registration of the Mark.

4.4 The Supplier shall not apply for, or obtain, registration of the Mark in any country for any goods or services.

4.5 The Supplier shall not apply for, or obtain, registration of any trade or service mark in any country which consists of, or comprises, or is confusingly similar to, the Mark for any goods or services.

5 Quality control

5.1 The Supplier shall comply with the specifications and standards relating to the Brand Licensed Products or Services which are specified in the Contract.

5.2 The Supplier shall promptly provide the Authority with copies of all communications relating to the Mark with any regulatory, industry or other authority.

5.3 The Supplier shall permit, and shall use its best endeavours to obtain permission for, the Authority at all reasonable times and on reasonable notice to enter any place used for the production, storage or distribution of the Marked Materials to inspect the Marked Materials in relation to compliance with this T Level Trade Mark Licence.

5.4 Without prejudice to any other rights of the Authority, in the event that the Authority finds that any sample of Marked Materials does not meet the requirements of this T Level Trade Mark Licence, it may give notice to the Supplier, and the Supplier shall take all reasonable steps to correct any deficiency as soon as reasonably practicable (having regard to constraints of the academic timetable).

6 Marketing, advertising and promotion

6.1 The Supplier undertakes to ensure that its advertising, marketing and promotion of Brand Licensed Products or Services shall in no way reduce or diminish the reputation, image and prestige of the Mark.

7 Recordal of licence

7.1 The Authority may, at its own cost, record the licence granted to it in paragraph 2 in the relevant registries against any registrations and applications for registration of the Marks.

7.2 The Supplier shall, at the Authority's request, execute a formal licence in such form and provide such other assistance as may be required for the purpose of such recordal.

8 Protection of the Mark

8.1 The Supplier shall immediately notify the Authority in writing giving full particulars if any of the following matters come to its attention:

8.1.1 any actual, suspected or threatened infringement of the Mark;

8.1.2 any actual or threatened claim that the Mark is invalid;

8.1.3 any actual or threatened opposition to the Mark;

8.1.4 any claim made or threatened that use of the Mark infringes the rights of any third party;

8.1.5 any person applies for, or is granted, a registered trade mark by reason of which that person may be, or has been, granted rights which conflict with any of the rights granted to the Supplier under this T Level Trade Mark Licence; or

8.1.6 any other form of attack, charge or claim to which the Mark may be subject.

8.2 In respect of any of the matters listed in paragraph 8.1:

8.2.1 the Authority shall, in its absolute discretion, decide what action if any to take;

8.2.2 the Authority shall have exclusive control over, and conduct of, all claims and proceedings;

8.2.3 the Supplier shall not make any admissions other than to the Authority and shall provide the Authority with all assistance that it may reasonably require in the conduct of any claims or proceedings; and

8.2.4 the Authority shall bear the cost of any proceedings and shall be entitled to retain all sums recovered in any action for its own account.

8.3 The provisions of section 30 of the Trade Marks Act 1994 (or equivalent legislation in any jurisdiction) are expressly excluded.

8.4 Nothing in this T Level Trade Mark Licence shall constitute any representation or warranty that:

8.4.1 any registration comprised in the Mark is valid;

8.4.2 any application comprised in the Mark shall proceed to grant or, if granted, shall be valid; or

8.4.3 the exercise by the Supplier of rights granted under this T Level Trade Mark Licence will not infringe the rights of any person.

9 Liability, indemnity and insurance

9.1 Nothing in this paragraph shall impose or create any liability of the Supplier to the Authority for use in England of the Mark on or in respect of Mandatory Marked Materials in accordance with the terms of this T Level Trade Mark Licence.

9.2 To the fullest extent permitted by law, the Authority shall not be liable to the Supplier for any costs, expenses, loss or damage (whether direct, indirect or consequential, and whether economic or other loss of profits, business or goodwill) arising from the Supplier's exercise of the rights granted to it under this T Level Trade Mark Licence.

9.3 Save as provided in paragraph 9.1, the Supplier indemnifies the Authority against all Loss to the Authority arising out of or in connection with the Supplier's exercise of its rights granted under this T Level Trade Mark Licence, including any claim made against the Authority for actual or alleged infringement of a third party's intellectual property rights arising out of or in connection therewith, other than where any such Loss and/or claim arises exclusively from the use of the Mark in accordance with this T Level Trade Mark Licence.

10 Additional Supplier obligations

10.1 The Supplier shall:

10.1.1 only make use of the Mark for the purposes authorised in this T Level Trade Mark Licence; and

10.1.2 comply with all regulations and practices in force or use in any territory to safeguard the Authority's rights in the Mark.

10.2 The Supplier shall not, nor directly or indirectly assist any other person to:

10.2.1 use the Mark except as permitted under this T Level Trade Mark Licence; or

10.2.2 do or omit to do anything to diminish the rights of the Authority in the Mark or impair any registration of the Mark.

10.3 The Supplier acknowledges and agrees that the exercise of the licence granted to the Supplier under this T Level Trade Mark Licence is subject to all applicable laws, enactments, regulations and other similar instruments in any territory, and the Supplier understands and agrees that it shall at all times be solely liable and responsible for such due observance and performance.

11 Sub-licensing

11.1 The Supplier shall have the right to grant to Approved Providers a sub-licence of any of its rights under this T Level Trade Mark Licence provided that:

11.1.1 the Supplier shall ensure that the terms of any sub-licence are in writing and are substantially the same as the terms of this T Level Trade Mark Licence (except that the sub-licensee shall not have the right to sub-license its rights) and the Supplier shall provide the Authority with a copy of the sub-licence on request and the Authority may require that any such sublicence includes the Authority as a party, and that the Authority is entitled to enforce its terms;

11.1.2 all sub-licences granted shall terminate automatically on termination or expiry of this T Level Trade Mark Licence; and

11.1.3 the Supplier shall be liable for all acts and omissions of any sub-licensee in relation to such sub-licence and indemnifies the Authority against all Losses incurred or suffered by the Authority, or for which the Authority may become liable, (whether direct, indirect or consequential and including any economic loss or other loss of profits, business or goodwill) arising out of any act or omission of any sub-licensee in relation to such sub-licence, other than to the extent any such Losses arise exclusively from the use of the Mark in accordance with this T Level Trade Mark Licence.

12 Duration and termination

12.1 This T Level Trade Mark Licence shall commence on the Effective Date and shall continue for the Term.

12.2 Without affecting any other right or remedy available to it under this T Level Trade Mark Licence or the Contract, the Authority may terminate this T Level Trade Mark Licence in respect of any Brand Licensed Product or Service with immediate effect by giving notice to the Supplier if:

12.2.1 the Supplier commits a material breach of any term of this T Level Trade Mark Licence in respect of such Brand Licensed Product or Service which breach is irremediable, or (if such breach is remediable) fails to remedy that breach within a period of 7 days after being notified to do so;

12.2.2 the Supplier repeatedly breaches any of the terms of this T Level Trade Mark Licence in respect of relevant Brand Licensed Products or Services or Brand Licensed Materials in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this T Level Trade Mark Licence; or

12.2.3 the Supplier challenges the validity of the Mark.

For the purposes of paragraph 12.2.1, **material breach** means a breach that is serious in the widest sense or of any of the obligations set out in paragraphs 3, 4.3, 4.4, 4.5, 5, 6.1, 10.1 or 11.1. In deciding whether any breach is material no regard shall be had to whether it occurs by some accident, mishap, mistake or misunderstanding.

13 Consequences of termination

13.1 On expiry or termination of this T Level Trade Mark Licence for any reason and subject to any express provisions set out elsewhere in this T Level Trade Mark Licence:

13.1.1 all rights and licences granted pursuant to this T Level Trade Mark Licence shall cease;

13.1.2 the Supplier shall cease all use of the Mark save as set out in this paragraph 13;

13.1.3 the Supplier shall co-operate with the Authority in the cancellation of any licences registered pursuant to this T Level Trade Mark Licence and shall execute such documents and do all acts and things as may be necessary to effect such cancellation;

13.1.4 the Supplier shall promptly deliver up to the Authority (or at the Authority's option, destroy) at the Supplier's expense all copies of promotional material which is Marked Material or otherwise bears any Mark as a designation of origin; and

13.1.5 any provision of this T Level Trade Mark Licence that expressly or by implication is intended to come into or continue in force on or after termination or expiry of this T Level Trade Mark Licence shall remain in full force and effect.

13.2 Termination or expiry of this T Level Trade Mark Licence shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the T Level Trade Mark Licence which existed at or before the date of termination or expiry.

Schedule 16 Appendix 1

Brand Licensed Products or Services

Those products and services identified as such in the T Level Branding Guidelines.

Mandatory Marked Materials

All Key Materials and such other materials as are identified as such in the T Level Branding Guidelines.

Schedule 16

T Level Branding Guidelines

S16_GEN2W1_DSS_T_Level_Branding_Guidelines

T Level Branding Guidelines

(November 2023)

T Level Branding Guidelines

1 Introduction

1.1 T Levels are high-quality technical qualifications for 16 to 19-year olds which are approved and managed by the Institute for Apprenticeships and Technical Education (IfATE). The T Level brand has been devised to ensure that Government, Awarding Organisations, Employers, Suppliers, Providers (schools and colleges), Students, and others involved with the qualification, support and promote T Levels in a positive manner that inspires confidence.

1.2 IfATE's T Level Branding Guidelines, including supporting annexes (the 'Guidelines') are essential reference material for all Suppliers responsible for the delivery of the Technical Qualification (TQ) component of the T Level qualification.

1.3 For simplicity, the registered trade marks associated with the T Level brand are referred to in the Guidelines as the 'T Level Marks' and are as follows:

- The word 'T Level';
- The Department for Education's (DfE's) 'T Level' logo (in black);
- IfATE's name and accompanying flower logo (in blue and black as detailed within the IfATE brand guide); and
- the respective Supplier's corporate name and logo.

1.4 These Guidelines set out essential information as to how the T Levels Marks should be used in: a) TQ materials and b) other T Level communications including for marketing, advertising and promotional purposes.

1.5 These Guidelines are subject to reasonable development. They adopt many of the general principles which apply in relation to good branding practice, and where they are developed further IfATE intends that they will, in terms of general principles, be similar in many respects to commonly used branding guidelines.

2 General principles for use of the T Level Marks

2.1 When using the T Level Marks, Suppliers (and any other authorised users, such as Providers) must comply with these Guidelines (in addition to any other requirements of the TQ Contract and the IfATE brand guide).

2.2 The T Level Marks must be used by Suppliers on the front/landing/home page **only** of all Mandatory Marked Materials, key TQ documents and supporting resources (unless otherwise agreed by IfATE), in accordance with and in the form set out at **Annex 1**.

2.3 Nothing in these Guidelines is intended to restrict the use of the text mark 'T Level' where that use is necessary to indicate the intended purpose of a product or service and is in accordance with honest practices in industrial or commercial matters. (This does not apply, unless authorised and used in accordance with these Guidelines, to the use of the T Level logo.)

2.4 By way of example, use to describe the relevance or purpose of a text book or support materials for a specific technical education qualification forming part of a T Level is generally acceptable, but any such use which is liable to confuse third parties as to whether the relevant T Level is approved, managed or otherwise controlled by a party other than IfATE, or that the text book or support materials are endorsed and/or approved by IfATE would not be acceptable.

2.5 The Secretary of State for Education, or IfATE under delegation by the Secretary of State for Education, shall have the exclusive power to issue certificates of award and statements of achievement (and equivalent documents, excluding a breakdown of attainment) within the T Level Programme. It is intended that such documents will include the Supplier's name but not the Supplier's logo.

2.6 Suppliers must not issue any document bearing the title or name, or described or represented as, a 'certificate' or 'statement of achievement' or its substantial equivalent to which, or in respect of which, any T Level Mark is applied or used, or otherwise apply the T Level Marks to, or create an association with any T Level or TQ with any document or material bearing the title or name, or described or represented as, a 'certificate' or 'statement of achievement'" or its substantial equivalent.

2.7 Suppliers must use the T Level Marks on all *Mandatory Marked Materials* used in the operational delivery of the TQ. The documents classified as *Mandatory Marked Materials* are listed in **Annex 2.**

2.8 *Mandatory Marked Materials* should include a descriptive qualification name, as determined and/or mutually agreed by IfATE and the Supplier, in line with the TQ Contract and these Guidelines e.g. [technical qualification] in x [Pathway]".

2.9 Suppliers must ensure that it is clear that any T Level, or qualification associated with a T Level (such as the TQ), is a qualification approved and managed by IfATE. T Level Marks must not be used on any materials which relate to a T Level or TQ which has been wholly or partly superseded, unless the material is equally prominently identified as such.

2.10 Suppliers must, on request from IfATE, submit copies of any material where their name or branding, or any other trade marks or branding are used and/or in association with a T Level or a TQ.

2.11 Suppliers must not promote that, or give the impression that, any of its other qualifications - similar or equivalent – are linked to the TQ or T Level qualification i.e. other Level 2, 3 or 4 qualifications.

3 Intellectual Property Rights (IPR) and the TQ Contract

3.1 Full details of Suppliers' rights and responsibilities in respect of IPR are set out in the TQ Contract, and Suppliers should pay particularly close attention to clause 13 Intellectual Property Rights; Schedule 14 Form of Assignment and License; and Schedule 16 Logos and Trademarks – T Level Trade Mark Licence.

3.2 Providers engaged with the T Level qualification may use the T Level Marks but it is the responsibility of Suppliers to ensure that they comply with these Guidelines and the TQ Contract.

3.3 Suppliers should note that the T Level Marks are registered trade marks; any breach could lead to an action for trade mark infringement (as well as other consequences under the TQ Contract).

4 Advertising, marketing and promotion

4.1 Suppliers must ensure that any advertising, marketing and promotion products or services i.e. those activities outside the scope of the core TQ delivery component, do not undermine or diminish the reputation, image and prestige of the T Level Marks when used in any such aforementioned activity e.g. media advertising.

4.2 Suppliers may use the T Level Marks in relation to *Brand Licensed Products or Services* set out in **Annex 3**, in accordance with (and subject to) the terms of the TQ Contract and these Guidelines.

4.3 Suppliers must not give the impression that their visual identity is being used as a distinct brand, trade mark or designation of origin for any materials, including for activity defined as *Brand Licensed Products or Services.*

5 Style, positioning and form of T Level Marks

5.1 Suppliers must ensure that, except for the T Level Marks, no other trade marks, logos, banners or graphics are to be presented and/or affixed to any materials which relate to a T Level or TQ.

T Level Marks on TQ Materials

5.2 The T Level Marks should be included on the front page only of the TQ materials (whether in paper or digital form) in accordance with and in the form set out at **Annex 1**.

5.3 The T Level Marks should be acknowledged on the final page of the TQ materials (whether in paper or digital form) in accordance with and in the form set out at **Annex 1**.

T Level Marks on other T Level communications (including for marketing, advertising and promotional purposes)

Positioning/Layout:

5.4 T Level Marks may be represented in the form of a logo or graphic image ("**Logo Mark**"); or as an isolated word mark ("**Isolated Word Mark**"); or as a text or word mark[1] used within relevant text ("**Text Mark**") as described below. There are some common requirements in relation to each type of use (sections 6 to 8 - "No mixing", "Prominence" and "Acknowledgements") and some requirements which differ depending on the form in which Suppliers plan to use the mark (set out below).

5.5 Use of the word mark may also be made in oral form. The same principles should, so far as practicable, apply to oral use of any T Level Marks i.e. if appropriate, the respective changes being proposed are applied consistently.

5.6 Where it is used otherwise than in text form, the form in which the Supplier reproduces the logo or graphic should conform precisely to the logo and graphic forms designated by IfATE.

[1] Text form includes in spoken text

5.7 **Logo Mark**:

- Suppliers must use the Logo Mark in precisely the form and subject to any requirements set out in **Annex 1**;
- Suppliers must not change the colours, or skew, stretch or angle the logo, or distort, add a border or otherwise alter the logo in any way;
- Suppliers must ensure that the logos are always clearly separate from any other material, and in particular that it has a clear space surrounding the logos, as illustrated, specified or referenced at **Annex 1**.
- Suppliers must not resize the logo, unless resizing is permitted in accordance with these Guidelines.

5.8 **Isolated Word Mark**

- Suppliers must use the fonts and size ranges of font set out in or referenced in these Guidelines and/ or as otherwise specified by IfATE*;*
- Suppliers must use only the colours and weights set out in or referenced in these Guidelines and/ or as otherwise specified by IfATE;
- Suppliers must not use underlining;
- The words should have initial capitalisation (only) and no other punctuation etc. "T Level" is acceptable; "T LEVEL", "T level" or T-Level" are not acceptable; and
- Suppliers must not use the Isolated Word Mark as a watermark.

5.9 **Text Mark**:

- Suppliers must use the Text Mark in the same font as the surrounding text; and
- Suppliers must acknowledge its first use in the text as noted under paragraph 5.15 (Acknowledgement) of these Guidelines.

No mixing/combination/background use

5.10 Suppliers must ensure that the T Level Marks are always clearly separate from any other trade mark or name used in the same document. In particular:

- Suppliers must not use their trade mark mixed or combined with any other trade mark or name such that they could be seen or understood to be part of a single trade mark. For example, “the Mrs Blogs [Supplier] T Level” would not be acceptable use; and

- Suppliers must not combine a T Level Mark into a single logo or something which might be seen to be or have a unitary character. For example:

is not acceptable.

- The T Level Mark and a Supplier’s mark should not be combined into a single logo or something which might be seen to be or have a unitary character. For example:

is not acceptable.

- There should always be a clear separation between the T Level Mark and any other mark used by Suppliers or on any documents, and, when used as a logo or graphic, Suppliers should take account of any requirements for separation set out in these Guidelines.

5.11 Any use of a name given to the qualification element of a T Level (including any use of “TQ” as a reference to part of a T Level) should also only be such that it is always a clearly separate mark or name from any other trade mark or name used in the same document with any other trade mark or trade name.

5.12 Suppliers must not place a T Level Mark against a background colour, pattern or picture except as specified below:

- as set out in or referenced in **Annex 1** or as otherwise agreed in writing by IfATE or specified in these Guidelines; or

- with imagery which is of a purely illustrative character, and does not suggest any other source or business connection, and is appropriate to the context and brand identity, and allows the entire mark to be clearly visible more prominently than such imagery, and complies with any other limitations notified by IfATE in writing from time to time,

and in any event any imagery must be consistent with the overall brand identity and values of the T Level Marks and the T Level Programme, and not be liable to bring the T Level Marks or the T Level Programme into disrepute.

Prominence

5.13 Where Suppliers use the T Level Marks on material which carries other branding in conjunction with or in the same part of the material, the T Level Marks should be given at least equal prominence with the other branding. For example:

- it should appear in script of at least the same font size as the script of any Supplier's trade mark, and where Suppliers use a logo covering at least the same overall surface area;
- the style used for the other mark should not lead to it being more prominent than the style used for the T Level Mark;
- the colouring used for the other mark should not draw more attention to it than the T Level Mark; and
- it should appear in at least as prominent a position.

5.14 Typically, use of one T Level Mark will not be regarded as 'in conjunction' with another mark when they are in separate distinct parts of the document, including for example, use of a Supplier's letter head (one part) and use of the T Level Mark in the body of the letter (a separate part).

Acknowledgement

5.15 Subject to paragraph 5.16 of these Guidelines, where the T Level Marks are used in any document, Suppliers should place in the document reasonably prominently (so that it would reasonably be expected to come to the attention of the reader or addressee of the document) an acknowledgement that IfATE's name and logo are registered trade marks of IfATE. For example:

- where the T Level Mark is used in the title or opening description of the document or in a manner intended to show that the document relates to a T Level or a TQ, by using a referenced footnote acknowledging that 'T Level is a registered trade mark of The Institute for Apprenticeships and Technical Education' or 'Registered trade mark of The Institute for Apprenticeships and Technical Education';

- where it is used in the text of a document, the first time it appears it should include a referenced footnote acknowledging that the '[Mark] is a registered trade mark of The Institute for Apprenticeships and Technical Education' or 'Registered trade mark of The Institute for Apprenticeships and Technical Education';

- in each case the referenced footnote should, where practicable, appear in the same visual field as the use of the T Level Marks, or in other cases, where such notice would otherwise commonly be placed. For example, on the rear of a single page which is printed on both sides, on the rear of the front page of a booklet, or on the rear of the last page of a booklet; and

- where a Supplier's or a Provider's name or branding is also used in the document, the referenced footnote should also make clear that the T Level is a qualification approved and managed by IfATE, and that the Supplier is currently authorised by IfATE to develop and deliver the qualification (and/or that the Provider offers or provides courses for part of the T Level, which is a qualification approved and managed by IfATE), as appropriate.

5.16 Where a reference is made to T Level in any document indirectly (for example with a description which is evidently a reference to a T Level or the TQ) in association with a Supplier (whether using a Supplier's name or otherwise), the document should make clear that the T Level and a TQ is a qualification approved and managed by IfATE.

5.17 No further acknowledgement is necessary where the use of the T Level Marks or a reference to a T Level or TQ is in a document, other than those materials/document listed in **Annex 2** of these Guidelines. To illustrate: such use is in word form (as part of the text[2]) of the document and would clearly be understood by addressees and readers as being a reference to the T Level or, as appropriate and reference has been to the fact that the TQ is approved and managed by IfATE and it is not being suggested otherwise: it has been made clear that the role of the Supplier is focused on developing and/or delivering the TQ component of the T Level and it has a relationship with IfATE.

Illustrations

The approach may be adjusted sensibly for the particular materials and circumstances of use. For example:

5.18 On promotional documentation intended for Providers, where it might be expected that a high level of prominence would be given to a Supplier's name or branding (for example in large

[2] including spoken text in the case of spoken material

script), or on explanatory documentation intended for Providers, the use of T Level (and T Level Marks, including text marks) should be given equal prominence. In a referenced footnote should appear on the reverse of the first page (for example with other similar notices, such as copyright notices, but no less prominently than those notices);

5.19 For promotional and explanatory documentation aimed at students or employers, the use of T Level should be given equal prominence; and a clear note should appear on the same page in the same visual field that the T Level is a qualification approved and managed by IfATE, and a Supplier's development and delivery of the qualification and use of the mark is under the authority of IfATE;

5.20 For assessment or examination papers (for single use) relating to materials for examiners, a reasonably prominent note should appear at the bottom of the first page that the T Level is a qualification approved and managed by IfATE, and a Supplier's development and delivery of the qualification and use of the mark is under the authority of IfATE;

5.21 For sample papers which may be re-used, there should in addition be a note that T Level is a registered trade mark of IfATE; and

5.22 For any supplementary materials (such as text books and learning aids), other than those materials/ documents listed in Annex 2, there should be a clear reasonably prominent explanation that the material is designed for use with the relevant T Level; including the date of the T Level, and that the T Level is a qualification approved and managed by IfATE, and that the T Level is a registered trade mark of IfATE used by a Supplier (or other source) with the authority of IfATE.

Providers (Schools and Colleges)

5.23 Suppliers are responsible for ensuring that:

- each Provider complies with these marking requirements, as they apply to use of a Supplier's name or branding and equally, to any permitted use of the Provider's name or branding in association with the T Level Mark; and
- any use by a Provider of the T Level Mark is clearly a reference to a T Level approved and managed by IfATE.

6 Inspection and Approval

6.1 Suppliers must permit IfATE to inspect on reasonable request and on reasonable notice any materials bearing or intended to bear a T Level Mark, for the purposes of ascertaining compliance with these Guidelines.

6.2 Where IfATE determines (acting reasonably) that it appears that there is a non-compliance with these Guidelines, Suppliers must consult with IfATE on how such non-compliance may be remedied, taking into account both the seriousness of the non-compliance, including how the relevant material does not comply, what the potential impact may be (bearing in mind the volumes of material in question and the audience for those materials) and the potential impact of remedial steps, with a view to reaching fair and reasonable consensus on remedial action (which may range from taking steps in relation to future materials to the withdrawal and reissue of current materials).

6.3 In the event that no consensus can be reached, the disagreement or difference will be subject to the Dispute Resolution Procedure.

7 Amendments to the Guidelines

7.1 IfATE may amend these Guidelines from time to time, in a manner consistent with the general principles (Section 2).

7.2 IfATE will notify Suppliers of any changes together with the date on which such amendments are to take effect.

7.3 IfATE will take reasonable account of Suppliers' comments or concerns in relation to any amendments and the timetable for implementation, and Suppliers agree to act reasonably to seek a consensus. In the absence of consensus the disagreement or difference may be referred by Suppliers or IfATE to be resolved under the Dispute Resolution Procedure, as set out in Annex 4.

Annex 1 (a): T Level Marks on Mandatory Marked TQ materials

Front page

*

*to be placed top right within the header

Supplier logo]**

**to be placed bottom right within the footer

Final page

Annex 1 (b): T Level Marks on Marked TQ materials

Front page

T-LEVELS*

*to be placed top right within the header

[Supplier logo]**

**to be placed bottom right within the footer

Final page

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

[SUPPLIER] is authorised by the Institute for Apprenticeships and Technical Education to develop and deliver this Technical Qualification.

Annex 2: Mandatory Marked Materials

Key Materials

a) specifications of content for each TQ including core and all specialist components;
b) assessment guidelines (for Providers);
c) quality assurance requirements (for Providers);
d) specimen assessment materials;
e) standards exemplification materials;
f) updates or redevelopments of specifications of content;
g) updates and redevelopments of any Key Materials; and
h) any materials equivalent to the above to which a Skilled Future Supplier would reasonably require access for the Portability Purposes.

Key Materials shall **not** include support Materials, insofar as they are not part of any of the expressly included items listed above;

Ancillary Materials

a) Assessment Strategy;

Annex 3: Brand Licensed Products and Services

Marketing materials relating to T Levels

Suppliers will be expected to adhere to the form of branding as set out in Annex 1 wherever reasonably practicable.

Annex 4: Dispute Resolution Procedure

Definitions[3]

"**Dispute**" means any claim, dispute or difference which arises out of or in connection with these Guidelines or in connection with the existence, legal validity or enforceability of these Guidelines, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts.

"**Style**" means any matter set out in or referred to in paragraph 5 of the Guidelines.

"**Dispute Resolution Procedure**" means the dispute resolution procedure set out in paragraphs 1.1 to 1.5.

1 Resolving disputes

1.1 Where a Dispute (not being a Dispute arising solely in respect of Style):

1.1.1 arises solely between IfATE and a Supplier, the dispute resolution procedure set out in clause 37 of the Supplier's Contract shall apply and the provisions of this Dispute Resolution Procedure shall not apply; or

1.1.2 relates to or is in connection with a dispute that is progressing under the Supplier's Contract, the parties agree to be bound by the decision that is reached in accordance with the dispute resolution procedure set out in clause 37 of the Supplier's Contract in respect of the dispute under the Supplier's Contract, provided always that IfATE and/or the Supplier (as the case may be) have taken into account all reasonable comments and/or submissions of any third party who is a party to, or connected with, the Dispute.

1.2 Where the Dispute is one to which the circumstances described in paragraph 1.1 do not apply:

1.2.1 and the Dispute remains unresolved, the relevant parties connected with the Dispute shall procure that nominated senior representatives of each such party who have authority to settle the Dispute will, within 28 days of a written request from another connected party, meet in good faith to resolve the Dispute; and

1.2.2 if the Dispute is not resolved at that meeting, the relevant parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the Dispute. If the relevant parties

cannot agree on a mediator, the mediator with experience in trade mark law will be nominated by CEDR. If a relevant party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute:

(i) the Dispute (other than a Dispute relating to Style) must be resolved using paragraphs 1.3 to 1.5; or

(ii) a Dispute relating to Style must be resolved using paragraph 1.6.

1.3 Unless IfATE refers the Dispute (other than a Dispute relating to Style) to arbitration using paragraph 1.4, the parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction (other than in relation to a Dispute relating to Style) to:

1.3.1 determine the Dispute; and/or

1.3.2 grant interim remedies, or any other provisional or protective relief.

1.4 The parties agree that IfATE has the exclusive right to refer any Dispute (other than a Dispute relating to Style) to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

1.5 IfATE has the right to refer a Dispute (other than a Dispute relating to Style) to arbitration even if a party has started or has attempted to start court proceedings under paragraph 1.3, unless IfATE has agreed to the court proceedings or participated in them. Even if court proceedings have started, the relevant party must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under paragraph 1.4.

1.6 If the Dispute is one which relates to Style, IfATE's decision will be final.

Schedule 16 Appendix 2

Mark

T Level

Registered trade mark(s) and applications[3]

Country	Mark	App or regn no	Date of app or regn	Classes	Specification
UK	T Level (word)	UK00003318112	15 June 2018	9, 16, 41	Class 9: Electronic apparatus and instruments for testing, examination and assessment purposes; computer software, hardware and firmware for the provision of examination and assessments including software for operation over computer networks or by remote computer access; all of the aforesaid for use in the provision of education, teaching, training and/or assessment. Class 16: Examination papers; syllabi; diplomas; education, academic and vocational certificates; printed examination regulations; all of the aforesaid for use in the provision of education, teaching, training and/or assessment.

[3] To be updated as required based on trade mark application position at the Effective Date.

					Class 41: Issuing of educational awards; awarding of educational certificates; educational assessment services; provision of examination, testing and assessment services; provision of examination, testing and assessment services electronically, by online delivery, by way of the Internet or world wide web; online publication of syllabi, examination papers, assessments; examination services; assessment services; educational certification services; certification in relation to examinations and other forms of assessment; preparation and validation, accreditation, conducting and administration of examinations, assessments and tests; provision of examination papers; information, advisory and consultancy services relating to all of the aforesaid; all of the aforesaid relating to the provision of education, teaching, training and/or assessment.
EU	T Level (word)	017999579	13 December 2018	9, 16, 41	Class 9: Educational, teaching, instruction or research apparatus and instruments; electronic apparatus and instruments for teaching, instruction, training, research, education, testing, examination and assessment purposes; media bearing electronic publications and data; electronic publications; electronic publications (downloadable) provided online from a database or the Internet; downloadable text and information provided electronically, by online delivery, by way of the

					Internet or world wide web; electronic database; audio visual teaching apparatus; films and video films; computer software, hardware and firmware; computer software, hardware and firmware for the provision of teaching, instruction, training, research, education, testing, examination and assessments including software for operation over computer networks or by remote computer access; educational software; all of the aforesaid for use in the provision of education, teaching, training and/or assessment. Class 16: Printed publications; educational publications; printed matter; educational materials; examination papers; syllabi; diplomas; education, academic and vocational certificates; printed examination regulations; books; magazines; publications; textbooks; exercise books and notebooks; catalogues, handbooks and manuals; study guides; instructional or teaching materials; all of the aforesaid for use in the provision of education, teaching, training and/or assessment. Class 41: Education services; teaching services; publication services; educational publication services; publication of printed matter relating to education; issuing of educational awards; awarding of educational certificates; electronic publication; publication of printed matter; educational assessment services; provision of training, teaching,

					academic, education, instruction, examination, testing and assessment services; provision of training, teaching, academic, education, instruction, examination, testing and assessment services electronically, by online delivery, by way of the Internet or world wide web; online publication of electronic texts, books, textbooks, brochures, syllabi, examination papers, assessments; examination services; assessment services; educational certification services; certification in relation to examinations and other forms of assessment, education, training and awards; preparation and validation, accreditation, conducting and administration of examinations, assessments and tests; provision of examination papers; information, advisory and consultancy services relating to all of the aforesaid services; all of the aforesaid relating to the provision of education, teaching, training and/or assessment services.

Schedule 17

Provider Contract requirements

1 Provider Contract

1.1 This Schedule sets out the requirements that Provider Contracts must meet.

1.2 Provider Contracts must:

1.2.1 be in writing, enforceable, and on terms that are fair and reasonable;

1.2.2 set out all the requirements with which the Approved Provider must comply in order to continue to deliver the TQ;

1.2.3 establish a sanctions policy to be applied in the event that the Approved Provider fails to comply with the requirements in the Provider Contract;

1.2.4 require the Approved Provider to:

(i) take all reasonable steps to ensure that the Supplier is able to comply with its Conditions of Recognition;

(ii) retain a workforce of appropriate size and competence to undertake the delivery of the TQ as required by the Supplier;

(iii) have available sufficient managerial and other resources to enable it effectively and efficiently to undertake the delivery of the TQ as required by the Supplier;

(iv) undertake the delivery of the qualification required by the awarding organisation in accordance with the Equality Act 2010, any Act that was a statutory predecessor to that Act, or any legislation in a jurisdiction other than England which has an equivalent purpose and effect; and

(v) operate a complaints handling procedure or appeals process for the benefit of Students;

1.2.5 where, in accordance with the Approved Assessment Strategy an Approved Provider is permitted to carry out or procure the carrying out of marking of Student assessment evidence, set out details for carrying out Moderation;

1.2.6 not materially depart from any relevant industry standards and common education sector practices;

1.2.7 be materially consistent across all Approved Providers in respect of the provision of the Provider Services and, in particular, shall not discriminate against any particular types, sizes or geographical locations of Approved Providers in connection with the provision of any Provider Services;

1.2.8 include appropriate GDPR provisions: where the Supplier, in fulfilling its obligations under this Contract, is acting as a Processor on behalf of an Approved Provider, the Provider Contract will include provisions to ensure that any personal data (as defined in the GDPR) that is Processed by the Supplier in relation to the Provider Services is Processed in accordance with Data Protection Legislation;

1.2.9 be consistent with, and to the extent necessary allow for, any information, document and data sharing requirements contained within this Contract (to include any information, documents and data that must be provided by the Supplier to the Authority and/or any third party and any information, documents and data requested by Ofqual);

1.2.10 require the Approved Provider to assist the Supplier in carrying out any reasonable monitoring activities and to assist Ofqual in any investigations made for the purposes of performing its functions;

1.2.11 allow Approved Providers to purchase Provider Services on an “as and when needed” basis without any minimum or maximum volume commitments (including in relation to the number of Students);

1.2.12 require Approved Providers to register all Students on a TQ by the end of November or within such other timescales as are required by the Key Dates Schedule for the relevant Academic Year and pay that part of the Fees

referred to in limb (a) of the definition of Fees within 30 days of such registration and provide that, if a Student terminates their study of the TQ before the end of the following January in the same Academic Year, the Supplier must provide a full refund of such Fees (relating to such Student) to the Approved Provider (for the avoidance of doubt, if the Student terminates their study of the TQ after the end of the following January in the same Academic Year, the Supplier is not obliged to give a refund);

1.2.13 include detailed provisions relating to the Approved Provider's role in quality assurance, such provisions shall give effect to the requirements of the Approved Provider's Quality Assurance Process;

1.2.14 require Approved Providers to provide advice and guidance to Students (including any Student no longer enrolled with the Approved Provider) in relation to making enquiries about results (and any further steps that may be taken following such an enquiry (including those contemplated by the Additional Services)) and where such Student reasonably requests the Approval Provider (whether directly or indirectly) to request the provision of an Additional Service, require the Approved Provider to request the provision of such Additional Service from the Supplier;

1.2.15 require Approved Providers to seek written approval from the Supplier before permitting a third party (for example training providers or satellite centres) to deliver any part of the TQ, including its assessments, and requires the Approved Providers to agree in writing to the Supplier's requirements before the Supplier approves the use of a third party;

1.2.16 place responsibility on the Approved Provider to monitor whether any third party involved with the delivery and assessment of the TQ on its behalf has appropriate capacity and capability; and

1.2.17 specify a process to be followed in any withdrawal of the Approved Provider (whether voluntary or not) from its role in delivering the TQ and require Approved Providers to take all reasonable steps to protect the interests of Students in the case of such a withdrawal.

1.3 Provider Contracts must not:

1.3.1 include terms in connection with Provider Services that are not strictly necessary for the provision of the relevant Provider Services and/or which are materially inconsistent with any of the Supplier's obligations under this Contract;

1.3.2 make the provision of the Provider Services contingent on the take up of any further qualifications or services by the Approved Provider;

1.3.3 require the Approved Provider to make any payments other than the Fees (e.g. for the avoidance of doubt, Provider Contracts shall not require any fees to be paid by the Approved Provider (or an Eligible Provider) for Provider Approval in relation to a TQ);

1.3.4 offer any discounts to the Fees; and/or

1.3.5 include provisions that are materially more onerous than any comparable provisions in this Contract.

1.4 The Supplier shall not offer to any Approved Provider any rebate, discount or other incentive in relation to services outside the Provider Services (whether or not in the Provider Contract) which is contingent on or linked to the Approved Provider entering into the Provider Contract and/or registering Students for the TQ.

Schedule 18

Commercially Sensitive Information

The content for this Schedule is contained in a separate file at:

S18_GEN2W1_DSS_Commercially_Sensitive_Confidential_Information

Attachment 9: Commercially Sensitive Information and/or Confidential Information

1 All the information that the Authority supplies (to the Potential Supplier or otherwise) as part of this Procurement shall be treated as confidential information under paragraph 12 of the Terms of Participation.

2 a. During this Procurement, the Potential Supplier considers that the type of information listed in Table 1 below contained in its response to the ITT is 'Confidential Information'.

b. From the Effective Date of the Contract, the Potential Supplier considers that the type of information listed in Table 3 below contained in its response to the ITT shall be 'Confidential Information'.

3 a. During this Procurement, the Potential Supplier considers that the type of information listed in Table 2 below contained in its response to the ITT is not Confidential Information but is 'Commercially Sensitive Information'.

b. From the Effective Date of the Contract, the Potential Supplier considers that the type of information listed in Table 4 below contained in its response to the ITT is not Confidential Information but is 'Commercially Sensitive Information'.

4 The Potential Supplier must complete each Table fully and give full, valid and justifiable reasons for including any information in the Tables below. The Authority cannot accept any broad attempt to class all, or any broad categories of, information as either 'Confidential Information' or 'Commercially Sensitive Information' and may discard a Potential Supplier's attempts to classify information in this way.

5 The information supplied in this Attachment 9 shall be used to populate Schedule 18 of the Contract.

6 Potential Suppliers are reminded that notwithstanding the inclusion of any information in Table 1, Table 2, Table 3 and/or Table 4 below, the Authority shall be responsible for determining in its absolute discretion whether any information is exempt from disclosure in accordance with FoIA and/or the EIRs.

Schedule 19

Required Insurances

PART A: THIRD PARTY PUBLIC AND PRODUCTS LIABILITY INSURANCE

1 Insured

The Supplier

2 Interest

To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental:

2.1 death or bodily injury to or sickness, illness or disease contracted by any person; and

2.2 loss of or damage to property,

happening during the period of insurance (as specified in paragraph 5) and arising out of or in connection with the provision of the Services under this Contract.

3 Limit of indemnity

Not less than £5,000,000 in respect of any one occurrence, the number of occurrences being unlimited, but £5,000,000 in the aggregate per annum in respect of products and pollution liability.

4 Territorial limits

United Kingdom.

5 Period of insurance

From the Effective Date and renewable on an annual basis unless agreed otherwise by the Authority in writing for the Term.

6 Cover features and extensions

Indemnity to principals clause.

7 Principal exclusions

7.1 War and related perils.

7.2 Nuclear and radioactive risks.

7.3 Liability for death, illness, disease or bodily injury sustained by employees of the Insured during the course of their employment.

7.4 Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.

7.5 Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.

7.6 Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.

7.7 Liability arising from the ownership, possession or use of any aircraft or marine vessel.

7.8 Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

8 Maximum deductible threshold

Not to exceed £10,000 for each and every third party property damage claim (personal injury claims to be paid in full).

PART B: PROFESSIONAL INDEMNITY INSURANCE

1 Insured

The Supplier

2 Interest

To indemnify the Insured for all sums which the Insured shall become legally liable to pay (including claimants' costs and expenses) as a result of claims first made against the Insured during the period of insurance (as specified in paragraph 13) by reason of any negligent act, error and/or omission arising from or in connection with the provision of the Services.

3 Limit of indemnity

Not less than £5,000,000 in respect of any one claim and in the aggregate per annum, exclusive of defence costs which are payable in addition.

4 Territorial Limits

United Kingdom

5 Period of insurance

From the Effective Date and renewable on an annual basis unless agreed otherwise by the Authority in writing (a) for the Term; and (b) for a period of 6 years thereafter.

6 Cover features and extensions

Retroactive cover to apply to any “claims made policy wording” in respect of this Contract or retroactive date to be no later than the Effective Date.

7 Principal exclusions

7.1 War and related perils

7.2 Nuclear and radioactive risks

8 Maximum deductible threshold

Not to exceed £10,000 for each and every claim.

PART C: UNITED KINGDOM COMPULSORY INSURANCES

1 The Supplier shall meet its insurance obligations under applicable Law in full, including, UK employers' liability insurance and motor third party liability insurance.

Schedule 20

Authorised Representatives

The content for this Annex is contained in a separate file at:

S20_GEN2W1_DSS_Authorised_Representatives

Schedule 20

Authorised Representatives

Authority Authorised Representative

[redacted]	[redacted]
[redacted]	[redacted]
Postal Address:	Sanctuary Buildings, 20 Great Smith Street, London SW1P 3BT
[redacted]	[redacted]

Supplier Authorised Representative

[redacted]	[redacted]
[redacted]	[redacted]
Postal Address:	Pearson Education Ltd 80 Strand London WC2R 0RL
[redacted]	[redacted]

Schedule 21

Staff Transfer

1. **Definitions**

1.1 In this Schedule, the following definitions shall apply:

"Former Supplier" means the Awarding Organisation that is operating or operated the T Level technical education qualification under the Original Contract;

"Notified Sub-contractor" means a Sub-contractor to whom Transferring Former Supplier Employees will transfer on a Relevant Transfer Date;

"Replacement Sub-contractor" means a sub-contractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any sub-contractor of any such sub-contractor);

"Relevant Transfer" means a transfer of employment to which TUPE applies;

"Relevant Transfer Date" means in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place;

"Service Transfer" means any transfer of the Services (or any part of the Services), for whatever reason, from the Supplier or any Sub-contractor to a Replacement Supplier or a Replacement Sub-contractor;

"Service Transfer Date" means the date of a Service Transfer;

"Staffing Information" means in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Authority may reasonably request (subject to all applicable provisions of the Data Protection Legislation), but including in an anonymised format:

(a) their ages, dates of commencement of employment or engagement, gender and place of work;

(b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;

(c) the identity of the employer or relevant contracting Party;

(d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;

(e) their wages, salaries, bonuses and profit sharing arrangements as applicable;

(f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;

(g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);

(h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;

(i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and

(j) any other Employee Liability Information" as such term is defined in regulation 11 of TUPE;

"Supplier's Final Supplier Personnel List" means a list provided by the Supplier of all Supplier Personnel who will transfer under TUPE on the Service Transfer Date;

"Supplier's Provisional Supplier Personnel List" means a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;

"Transferring Former Supplier Employees" means in relation to a Former Supplier, those employees of the Former Supplier to whom TUPE will apply on the Relevant Transfer Date; and

"Transferring Supplier Employees" means those employees of the Supplier and/or the Supplier's Sub-contractors to whom TUPE will apply on the Service Transfer Date.

2. Interpretation

2.1 Where a provision in this Schedule imposes an obligation on the Supplier to provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to the Authority, Former Supplier, Replacement Supplier or Replacement Sub-contractor, as the case may be.

Transferring Former Supplier Employees at Commencement of Services

3. Relevant Transfers

3.1 The Authority and the Supplier agree that:

3.1.1 the commencement of the provision of the Services or of any relevant part of the Services will be a Relevant Transfer in relation to the Transferring Former Supplier Employees; and

3.1.2 as a result of the operation of TUPE, the contracts of employment between each Former Supplier and the Transferring Former Supplier Employees (except in relation to any terms disapplied through the operation of regulation 10 of TUPE) shall have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or Notified Sub-contractor and each such Transferring Former Supplier Employee.

3.2 The Authority shall procure that each Former Supplier shall comply with all its obligations under TUPE and shall perform and discharge all its obligations in respect

of all the Transferring Former Supplier Employees in respect of the period up to (but not including) the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions which in any case are attributable in whole or in part in respect of the period up to (but not including) the Relevant Transfer Date) and the Supplier shall make, and the Authority shall procure that each Former Supplier makes, any necessary apportionments in respect of any periodic payments.

4. <u>Former Supplier Indemnities</u>

4.1 Subject to Paragraph 4.2, the Authority shall procure that each Former Supplier shall indemnify the Supplier and any Notified Sub-contractor against any Employee Liabilities arising from or as a result of:

4.1.1 any act or omission by the Former Supplier in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in TUPE) of any Transferring Former Supplier Employee arising before the Relevant Transfer Date;

4.1.2 the breach or non-observance by the Former Supplier arising before the Relevant Transfer Date of:

(a) any collective agreement applicable to the Transferring Former Supplier Employees; and/or

(b) any custom or practice in respect of any Transferring Former Supplier Employees which the Former Supplier is contractually bound to honour;

4.1.3 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:

(a) in relation to any Transferring Former Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising before the Relevant Transfer Date; and

(b) in relation to any employee who is not a Transferring Former Supplier Employee and in respect of whom it is later alleged or determined that TUPE applied so as to transfer his/her employment from the Former Supplier to the Supplier and/or any Notified Sub-contractor as appropriate, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations in respect of the period to (but excluding) the Relevant Transfer Date;

4.1.4 a failure of the Former Supplier to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Former Supplier Employees in respect of the period to (but excluding) the Relevant Transfer Date;

4.1.5 any claim made by or in respect of any person employed or formerly employed by the Former Supplier other than a Transferring Former Supplier Employee for whom it is alleged the Supplier and/or any Notified Sub-contractor as appropriate may be liable by virtue of this Contract and/or TUPE; and

4.1.6 any claim made by or in respect of a Transferring Former Supplier Employee or any appropriate employee representative (as defined in TUPE) of any Transferring Former Supplier Employee relating to any act or omission of the Former Supplier in relation to its obligations under regulation 13 of TUPE, except to the extent that the liability arises from the failure by the Supplier or any Sub-contractor to comply with regulation 13(4) of TUPE.

4.2 The indemnities in Paragraph 4.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Sub-contractor whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities:

4.2.1 arising out of the resignation of any Transferring Former Supplier Employee before the Relevant Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Supplier or any Sub-contractor to occur in the period from (and including) the Relevant Transfer Date; or

4.2.2 arising from the failure by the Supplier and/or any Sub-contractor to comply with its obligations under TUPE.

4.3 If any person who is not identified as a Transferring Former Supplier Employee claims, or it is determined in relation to any person who is not identified as a Transferring Former Supplier Employee, that his/her contract of employment has been transferred from a Former Supplier to the Supplier and/or any Notified Sub-contractor pursuant to TUPE then:

4.3.1 the Supplier shall, or shall procure that the Notified Sub-contractor shall, within 5 Working Days of becoming aware of that fact, give notice in writing to the Authority and, where required by the Authority, to the Former Supplier; and

4.3.2 the Former Supplier may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification by the Supplier and/or the Notified Sub-contractor or take such other reasonable steps as the Former Supplier considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.

4.4 If an offer referred to in Paragraph 4.3.2 is accepted, or if the situation has otherwise been resolved by the Former Supplier and/or the Authority, the Supplier shall, or shall procure that the Notified Sub-contractor shall, immediately release the person from his/her employment or alleged employment.

4.5 If by the end of the 15 Working Day period specified in Paragraph 4.3.2:

4.5.1 no such offer of employment has been made;

4.5.2 such offer has been made but not accepted; or

4.5.3 the situation has not otherwise been resolved,

the Supplier and/or any Notified Sub-contractor may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

4.6 Subject to the Supplier and/or any Notified Sub-contractor acting in accordance with the provisions of Paragraphs 4.3 to 4.5 and in accordance with all applicable proper employment procedures set out in Law, the Authority shall procure that the Former

Supplier indemnifies the Supplier and/or any Notified Sub-contractor (as appropriate) against all Employee Liabilities arising out of the termination of employment pursuant to the provisions of Paragraph 4.5 provided that the Supplier takes, or shall procure that the Notified Sub-contractor takes, all reasonable steps to minimise any such Employee Liabilities.

4.7 The indemnity in Paragraph 4.6:

4.7.1 shall not apply to:

(a) any claim for:

(b) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or

(c) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees;

(d) in any case in relation to any alleged act or omission of the Supplier and/or any Sub-contractor; or

(e) any claim that the termination of employment was unfair because the Supplier and/or Notified Sub-contractor neglected to follow a fair dismissal procedure; and

4.7.2 shall apply only where the notification referred to in Paragraph 4.3.1 is made by the Supplier and/or any Notified Sub-contractor (as appropriate) to the Authority and, if applicable, the Former Supplier, within 6 months of the Relevant Transfer Date.

4.8 If any such person as is described in Paragraph 4.3 is neither re-employed by the Former Supplier nor dismissed by the Supplier and/or any Notified Sub-contractor within the time scales set out in Paragraph 4.5, such person shall be treated as having transferred to the Supplier or Notified Sub-contractor and the Supplier shall comply with such obligations as may be imposed upon it under the Law.

5. Supplier Indemnities and Obligations

5.1 Subject to Paragraph 5.2, the Supplier shall indemnify the Authority and/or the Former Supplier against any Employee Liabilities arising from or as a result of:

5.1.1 any act or omission by the Supplier or any Sub-contractor in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in TUPE) of any Transferring Former Supplier Employee whether occurring before, on or after the Relevant Transfer Date;

5.1.2 the breach or non-observance by the Supplier or any Sub-contractor on or after the Relevant Transfer Date of:

(a) any collective agreement applicable to the Transferring Former Supplier Employee; and/or

(b) any custom or practice in respect of any Transferring Former Supplier Employees which the Supplier or any Sub-contractor is contractually bound to honour;

5.1.3 any claim by any trade union or other body or person representing any Transferring Former Supplier Employees arising from or connected with any failure by the Supplier or a Sub-contractor to comply with any legal obligation to such trade union, body or person arising on or after the Relevant Transfer Date;

5.1.4 any proposal by the Supplier or a Sub-contractor prior to the Relevant Transfer Date to make changes to the terms and conditions of employment or working conditions of any Transferring Former Supplier Employees to their material detriment on or after their transfer to the Supplier or a Sub-contractor (as the case may be) on the Relevant Transfer Date, or to change the terms and conditions of employment or working conditions of any person who would have been a Transferring Former Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of TUPE) before the Relevant Transfer Date as a result of or for a reason connected to such proposed changes;

5.1.5 any statement communicated to or action undertaken by the Supplier or a Sub-contractor to, or in respect of, any Transferring Former Supplier Employee

before the Relevant Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Authority and/or the Former Supplier in writing;

5.1.6 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:

(a) in relation to any Transferring Former Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date; and

(b) in relation to any employee who is not a Transferring Former Supplier Employee, and in respect of whom it is later alleged or determined that TUPE applied so as to transfer his/her employment from the Former Supplier to the Supplier or a Sub-contractor, to the extent that the proceeding, claim or demand by the HMRC or other statutory authority relates to financial obligations arising on or after the Relevant Transfer Date;

5.1.7 a failure of the Supplier or any Sub-contractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Former Supplier Employees in respect of the period from (and including) the Relevant Transfer Date;

5.1.8 any claim made by or in respect of a Transferring Former Supplier Employee or any appropriate employee representative (as defined in TUPE) of any Transferring Former Supplier Employee relating to any act or omission of the Supplier or any Sub-contractor in relation to obligations under regulation 13 of TUPE, except to the extent that the liability arises from the Former Supplier's failure to comply with its obligations under regulation 13(4) of TUPE; and

5.1.9 a failure by the Supplier or any Sub-Contractor to comply with its obligations under Paragraph 2.8 above.

5.2 The indemnities in Paragraph 5.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Former Supplier whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Former Supplier's failure to comply with its obligations under TUPE.

5.3 The Supplier shall comply, and shall procure that each Sub-contractor shall comply, with all its obligations under TUPE (including without limitation its obligation to inform and consult in accordance with regulation 13 of TUPE) and shall perform and discharge, and shall procure that each Sub-contractor shall perform and discharge, all its obligations in respect of all the Transferring Former Supplier Employees, on and from the Relevant Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and any other sums due under the Admission Agreement which in any case are attributable in whole or in part to the period from (and including) the Relevant Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between the Supplier and the Former Supplier.

6. Information

6.1 The Supplier shall, and shall procure that each Sub-contractor shall, promptly provide to the Authority and/or at the Authority's direction, the Former Supplier, in writing such information as is necessary to enable the Authority and/or the Former Supplier to carry out their respective duties under regulation 13 of TUPE. The Authority shall procure that the Former Supplier shall promptly provide to the Supplier and each Notified Sub-contractor in writing such information as is necessary to enable the Supplier and each Notified Sub-contractor to carry out their respective duties under regulation 13 of TUPE.

7. Procurement Obligations

7.1 Notwithstanding any other provisions of this Schedule, where in this Schedule the Authority accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Authority's contract with the Former Supplier contains a contractual right in that regard

which the Authority may enforce, or otherwise so that it requires only that the Authority must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

8. Pensions

8.1 The Supplier shall, and shall procure that each Sub-contractor shall, comply with the requirements of Part 1 of the Pensions Act 2008, section 258 of the Pensions Act 2004 and the Transfer of Employment (Pension Protection) Regulations 2005 for all transferring staff.

DATED _____

THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION

and

PEARSON EDUCATION LIMITED

INTELLECTUAL PROPERTY ASSIGNMENT AND LICENCE IN RELATION TO THE DIGITAL: DIGITAL SUPPORT SERVICES T LEVEL TECHNICAL QUALIFICATION

THIS ASSIGNMENT AND LICENCE is made on

BETWEEN:

(3) **THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION** of Sanctuary Buildings, 20 Great Smith Street, London SW1P 3BT ("**Authority**"); and

(4) **PEARSON EDUCATION LIMITED**, a company registered in England and Wales (company registration number: **00872828**), whose registered office is at **Hailey Court, Jordan Hill Business Park, Oxford, OX2 8EJ** ("**Supplier**"),

each a "**Party**" and together the "**Parties**".

BACKGROUND TO THIS ASSIGNMENT AND LICENCE

(D) The Authority and the Supplier have entered into a contract on the date of this Assignment and Licence for the design, development and delivery of the technical education qualification element ("**TQ**") for the **Digital Support Services** T Level ("the **TQ Agreement**").

(E) The Supplier has agreed to assign certain intellectual property rights to the Authority, and to licence certain intellectual property rights to the Authority in connection with the TQ. The Authority has agreed to grant a licence back to the Supplier in relation to certain assigned intellectual property rights.

(F) This Assignment and Licence, together with the TQ Agreement sets out the agreed terms of such assignment and licences.

2 <u>Assignment and Licence start, formation and interpretation</u>

2.1 This Assignment and Licence is legally binding from the Effective Date until it ends in accordance with its terms.

2.2 In this Assignment and Licence, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this clause 1 or, where no definition is given in this clause 1, Schedule 1 to the TQ Agreement.

2.3 If a capitalised expression does not have an interpretation in this clause 1 or Schedule 1 to the TQ Agreement, it shall, in the first instance, be interpreted in accordance with the common

interpretation within the relevant market sector where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

2.4 In this Assignment and Licence, unless the context otherwise requires:

2.4.1 the singular includes the plural and vice versa;

2.4.2 reference to a gender includes the other gender and the neuter;

2.4.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

2.4.4 references to a legal entity (other than the Supplier) shall include unless otherwise expressly stated any statutory successor to such entity and/or the relevant functions of such entity, and references to the Department shall include, where relevant, the ESFA;

2.4.5 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

2.4.6 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

2.4.7 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

2.4.8 references to "**clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of this Assignment and Licence and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

2.4.9 references to "**paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and

2.4.10 the headings in this Assignment and Licence are for ease of reference only and shall not affect the interpretation or construction of this Assignment and Licence.

2.5 In this Assignment and Licence, unless the context otherwise requires, the following words shall have the following meanings:

"**Ancillary Materials**" means all information and materials (other than Key Materials) to which the Authority and/or a Future Supplier would require access for the Portability Purposes, and any other materials which would be required on or to facilitate succession to a Future Supplier in a seamless manner in relation to the TQ offered or Operated by the Supplier.

Ancillary Materials shall include, without limitation:

(a) Student results including grades;

(b) statistical analysis for grading (excludes the systems supporting the analysis);

(c) lists of Providers;

(d) marked Student evidence (with moderation outcomes);

(e) documentation which provides an overview or analysis of Student performance (including chief examiner and chief moderator reports), which include but are not limited to, examples of student responses to assessment questions and/or tasks as well as narrative explaining why students did well/ less well on individual items/ components/ subcomponents);

(f) data on Student credits;

(g) data on Student appeals;

(h) data on special considerations for Students;

(i) the Assessment Strategy;

(j) Student registrations;

(k) draft materials in preparation for forthcoming assessments;

(l) the Key Dates Schedule (in respect of forthcoming assessments);

(m) lists, with contact details, of people contracted by the Supplier to perform or oversee activities which are necessary for the conduct and quality assurance of assessments for the TQ;

(n) materials from completed assessments, such as completed Students' examination answer booklets; and

(o) TQ Live Assessment Materials

"**Approval**" has the same meaning as in the TQ Agreement;

"**Assigned Rights**" means the Intellectual Property Rights in the Key Materials;

"**Authority Authorised Representative**" has the same meaning as in the TQ Agreement;

"**Background IPR**" means any IPR owned by a Party prior to the Effective Date or created or developed by a Party otherwise than in the provision of the Services or under or in connection with the TQ Agreement, but does not include IPR in Key Materials;

"**Beneficiary**" means a Party having (or claiming to have) the benefit of an indemnity under this Assignment and Licence;

"**Claim**" means any claim for which it appears that a Beneficiary is, or may become, entitled to indemnification under this Assignment and Licence;

"**Continuing Activities**" means activities of the Supplier under the TQ Agreement which continue following the end of the second Academic Year for the final Exclusive Cohort (each as defined in the TQ Agreement) in relation to the TQ as offered by the Supplier, such as retakes, appeals, and any ongoing records management contracted to the Supplier;

"**Default**" means any breach of the obligations of the Supplier (including abandonment of the Assignment and Licence in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of this Assignment and Licence and in respect of which the Supplier is liable to the Authority;

"**Deliverables**" means all information and data the Supplier creates, identifies for use, or uses as part of or for the Operation of the TQ, including Products and Management Information;

"**Dispute**" means any claim, dispute or difference which arises out of or in connection with this Assignment and Licence or in connection with the negotiation, existence, legal validity, enforceability or termination of this Assignment and Licence, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;

"**Effective Date**" means the date on which the last Party to sign has signed this Assignment and Licence;

"**Final Approval Milestone**" has the meaning given in the TQ Agreement;

"**Future Supplier**" means any Awarding Organisation appointed, at any point in the future and including any Replacement Supplier, to operate one or more T Level technical education qualifications by or at the direction of the Authority from time to time, and where the Authority is operating a T Level technical education qualification, shall also include the Authority;

"**Indemnifier**" means a Party from whom an indemnity is sought under this Assignment and Licence;

"**Insolvency Event**" means:

(d) in respect of a company:

(i) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or

(ii) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or

(iii) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or

(iv) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or

(v) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or

(vi) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or

(vii) being a "**small company**" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

(e) where the person is an individual or partnership, any event analogous to those listed in limbs (a) (i) to (vii) (inclusive) occurs in relation to that individual or partnership; or

(f) any event analogous to those listed in limbs (a) (i) to (vii) (inclusive) occurs under the law of any other jurisdiction;

"**Intellectual Property Rights**" or "**IPR**" means:

(g) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;

(h) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(i) all other rights having equivalent or similar effect in any country or jurisdiction;

"**IPR Claim**" means any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR used to provide the Services and/or supply the Products or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority in the fulfilment of its obligations under the TQ Agreement or this Assignment and Licence;

"**Key Materials**" means materials the IPR in which the Authority reasonably requires ownership of for the Portability Purposes. Examples of where the Authority may reasonably require ownership include because the Authority or a Future Supplier (or, where relevant, a potential Future Supplier) may need to copy or otherwise reproduce such materials (in whole or in part), to supply or communicate the same, or to be able control the use (in whole or in part) of such materials by third parties, or to authorise others to do so.

Key Materials shall include:

(a) specifications of content for each TQ including core and all specialist components;

(b) assessment guidelines (for Providers);

(c) quality assurance requirements (for Providers);

(d) specimen assessment materials;

(e) standards exemplification materials;

(f) supplementary specimen assessment materials

(g) employer set project guide exemplar responses

(h) employer set project grade exemplar responses

(i) updates or redevelopments of specifications of content;

(j) updates and redevelopments of any Key Materials; and

(k) any materials equivalent to the above to which a Skilled Future Supplier would reasonably require access for the Portability Purposes.

Key Materials shall not include:

(1) Support Materials, insofar as they are not part of any of the expressly included items listed above;

(2) question banks insofar as they are not part of any of the included items listed above and are not developed for the TQ; and

(3) any systems and platforms used to support the delivery of the TQ, provided that the relevant TQ content or data held in or processed by such systems and/or platforms can be extracted without requiring further processing post-extraction (and the Supplier can demonstrate that they can be so extracted) to enable use of the relevant content and/or data by a Skilled Future Supplier in conjunction with a non-proprietary or generally commercially available system or platform;

"**Know-How**" means all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Services;

"**Law**" means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;

"**Losses**" means all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;

"**New IPR**" means :

(a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of the TQ Agreement and updates and amendments of these items including (but not limited to) database schema; and/or

(b) IPR in or arising as a result of the performance of the Supplier's obligations under the TQ Agreement and all updates and amendments to the same,

but shall not include any IPR owned by the Supplier prior to the Effective Date;

"**Operate**" in relation to a qualification means to provide the Services or a material part of the Services, or services replacing the Services or a material part of the Services, or of an equivalent character to the Services or a material part of the Services in relation to any other qualification (whether a T Level technical education qualification or not); and "**Operation**" and other cognate terms shall have a corresponding meaning;

"**Party**" means the Authority or the Supplier and "**Parties**" means both of them where the context permits;

"**Product**" has the meaning given in the TQ Agreement;

"**Provider**" means an organisation that has a grant agreement and/or a contract in place with the ESFA to provide qualifications to Students;

"**Replacement Services**" means any services which are substantially similar to any of the Services (including the supply of any Products) and which the Authority receives in substitution for any of the Services, whether those services are provided by the Authority internally and/or by any third party;

"**Replacement Supplier**" has the meaning given in the TQ Agreement;

"**Required Insurances**" has the meaning given in the TQ Agreement;

"**Services**" means the services as described in Schedule 2 to the TQ Agreement (*Service Requirements*) including any Additional Services as defined in the TQ Agreement;

"**Termination Notice**" means a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Assignment and Licence on a specified date and setting out the grounds for termination;

"**Third Party IPR**" means Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Services and/or supplying the Products;

"**TQ Agreement**" has the meaning given in recital A (above);

"**Transparent**" means that students and employers will regard the TQ delivered by a Future Supplier as materially the same as the TQ delivered and operated by the (existing) Supplier;

"**Working Day**" means any day other than a Saturday or Sunday or public holiday in England and Wales.

3 Assignment

3.1 Pursuant to and for the consideration set out in the TQ Agreement, the Supplier assigns to the Authority, absolutely with full title guarantee all its right, title and interest in and to all of the

Intellectual Property Rights in the Key Materials (which, for the avoidance of doubt, includes the Guide Standard Exemplification Materials) including the right to bring, make, oppose, defend, appeal proceedings, claims or actions and obtain relief (and to retain any damages recovered) in respect of any infringement, or any other cause of action arising from ownership, of any of the Assigned Rights on or after the date of this Assignment and Licence. Such assignment shall take place on the earlier of:

3.1.1 the creation of any relevant materials known to be Key Materials;

3.1.2 the identification by the Supplier of the use of the relevant materials as part of the TQ; and

3.1.3 delivery of the relevant Key Materials to the Authority, or Operation of the TQ by the Supplier.

3.2 With the exception of Guide Standard Exemplification Materials, all Key Materials are relevant course documents for the purposes of section A2D3(4) of the Apprenticeships, Skills, Children and Learning Act 2009, and on approval of the TQ at the Final Approval Milestone and on any subsequent Approval, to the extent that any copyright or any rights in copyright forming part of the Assigned Rights have not then been assigned to and vested absolutely in the Authority, they shall be transferred to the Authority by operation of statute in accordance with section A2IA of the Apprenticeships, Skills, Children and Learning Act 2009. Intellectual Property Rights in the Guide Standard Exemplification Materials is assigned to the Authority by virtue of 2.1 above.

4 Licences to the Authority

4.1 The Supplier hereby grants to the Authority (and the Authority shall have, in addition to any retained rights under clause 13.8 of the TQ Agreement) a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, exploit and sub-license the IPR in the Ancillary Materials and the Supplier's Background IPR and, in respect of any IPR in Key Materials, in each case to the extent that the same are not at the relevant time vested absolutely in the Authority, as necessary to enable the Authority (and its sub-licensees) to:

4.1.1 use the Key Materials and Ancillary Materials in its administration, approval and oversight of the TQ and other T Level technical education qualifications and to make the same available to others (such as Ofqual) to do the same; and

4.1.2 to use the Key Materials and the Ancillary Materials, and for any Future Supplier or potential Future Supplier to use the Key Materials and the Ancillary Materials:

(i) for competing or tendering for the delivery and Operation of the TQ and/or any Replacement TQ, during any Transition Period and following expiry or termination of the TQ Agreement; and

(ii) to deliver and Operate the TQ and any Replacement TQ, during any Transition Period and following expiry or termination of the TQ Agreement; and

4.1.3 otherwise to receive and use the Services and the Deliverables and allow any Future Supplier to use the Deliverables; and

4.1.4 to sub-license others to exercise the rights set out in this clause 3.1.

4.2 The Authority agrees that it shall use any Ancillary Materials which fall solely within element (I) of the definition of Ancillary Materials (being "*lists, with contact details, of people contracted by the Supplier to perform or oversee activities which are necessary for the conduct and quality assurance of assessments for the TQ*") only for the purposes of planning for or executing an Emergency Exit.

5 Licence to the Supplier

5.1 The Authority hereby grants to the Supplier, in respect of the Assigned Rights, a worldwide, royalty free, perpetual and irrevocable non-exclusive licence, with the right to sublicense, to use and exploit the IPR in the Key Materials during and after the Term, but not, save as provided in the TQ Agreement, to use the same as part of a T Level, such licence being subject to clauses 13.13 and 13.14 of the TQ Agreement (which for these purposes shall survive any termination or expiry of the TQ Agreement).

6 Warranties and representations

6.1 The Supplier warrants and represents (on the Effective Date and on any relevant assignment or grant of licence taking effect) that:

6.1.1 it is or will be the sole legal and beneficial owner of, and that it owns all the rights and interests in the Assigned Rights no later than the time for assignment specified in clause 2.1 or when they are assigned in accordance with clause 13.2.1 of the TQ Agreement, save for Assigned Rights other than New IPR, in respect of which it has previously

notified the Authority and the Authority has agreed in writing that this warranty shall not apply;

6.1.2 where it is not the sole legal and beneficial owner of the Assigned Rights, including the Assigned Rights which are to be used or embodied in any Key Materials, it has established that all owners of such rights consent to their assignment and transfer absolutely to the Authority;

6.1.3 it has all the necessary right and title to grant all the licences granted to the Authority under this Assignment and Licence and the TQ Agreement;

6.1.4 it has not licensed or assigned any of the Assigned Rights other than pursuant to this Assignment and Licence or the TQ Agreement;

6.1.5 the Assigned Rights are free from any security interest, option, mortgage, charge or lien;

6.1.6 it is unaware of any infringement or likely infringement of any of the Assigned Rights;

6.1.7 as far as it is aware, all the Assigned Rights are valid and subsisting and there are and have been no claims, challenges, disputes or proceedings, pending or threatened, in relation to the ownership, validity or use of any of the Assigned Rights;

6.1.8 the use of the Key Materials and Ancillary Materials, and exploitation of the Assigned Rights by the Supplier in the provision of the Services and Deliverables or by the Authority in receiving and using the Services and Deliverables or procuring any Replacement Services or by any Future Supplier in Operating any Replacement Services, will not infringe the rights of any third party; and

6.1.9 the Key Materials are its original work and have not been copied wholly or substantially from any other source.

7 Indemnity

7.1 Subject to clause 19, if there is an IPR Claim, the Supplier indemnifies the Authority against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

7.2 If an IPR Claim is made or anticipated, the Supplier must at its own expense and the Authority's sole option, either:

7.2.1 obtain for the Authority the rights in clause 2.1 and 3.1 without infringing any Third Party IPR; or

7.2.2 replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.

8 Moral rights

8.1 The Supplier shall procure written absolute waivers from all authors of the Key Materials and Ancillary Materials in relation to all their moral rights arising under the Copyright, Designs and Patents Act 1988 in relation to the Key Materials and Ancillary Materials and, as far as is legally possible, any broadly equivalent rights such authors may have in any territory of the world.

9 Ending or extending the Assignment and Licence

9.1 This Assignment and Licence ends if terminated by the Authority for any reason set out in this Assignment and Licence.

9.2 If any of the following events happen, the Authority has the right to immediately terminate this Assignment and Licence or any of the licences granted under this Assignment and Licence by issuing a Termination Notice to the Supplier (in the latter case specifying the relevant licences):

9.2.1 a Default incapable of remedy;

9.2.2 a Default capable of remedy that is not corrected within 30 days; and

9.2.3 anything occurs which entitles the Authority to terminate the TQ Agreement.

10 Claims against third parties

10.1 The Supplier may take any action it considers appropriate or necessary, subject to the Authority's prior written consent, not to be unreasonably withheld or delayed, if there is a breach, other than in connection with the TQ, by a third party of the Authority's rights in any IPR licensed to the Supplier under clause 4, and the Authority agrees to provide all such assistance as the Supplier may reasonably require (subject to meeting the Authority's reasonably agreed costs and expenses

and the Supplier hereby indemnifying the Authority in respect of any loss, damage or liability the Authority incurs by reason of any such action).

11 Further assurance

11.1 At the Authority's expense the Supplier shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this Assignment and Licence and the TQ Agreement, including:

11.1.1 registration of the Authority as applicant or (as applicable) proprietor of the Assigned Rights; and

11.1.2 assisting the Authority in obtaining, defending and enforcing the Assigned Rights, and assisting with any other proceedings which may be brought by or against the Authority against or by any third party relating to the Assigned Rights.

11.2 The Supplier appoints the Authority to be its attorney in its name and on its behalf to execute documents, use the Supplier's name and do all things which are necessary or desirable for the Authority to obtain for itself or its nominee the full benefit of this Assignment and Licence.

11.3 This power of attorney is irrevocable and is given by way of security to secure the performance of the Supplier's obligations under this Assignment and Licence and the proprietary interest of the Authority in the Assigned Rights and so long as such obligations of the Supplier remain undischarged, or the Authority has such interest, the power may not be revoked by the Supplier, save with the consent of the Authority.

11.4 Without prejudice to clause 10.2, the Authority may, in any way it thinks fit and in the name and on behalf of the Supplier:

11.4.1 take any action that this Assignment and Licence requires the Supplier to take;

11.4.2 exercise any rights which this Assignment and Licence gives to the Supplier; and

11.4.3 appoint one or more persons to act as substitute attorney(s) for the Supplier and to exercise such of the powers conferred by this power of attorney as the Authority thinks fit and revoke such appointment.

11.5 The Supplier undertakes to ratify and confirm everything that the Authority and any substitute attorney does or arranges or purports to do or arrange in good faith in exercise of any power granted under this clause 10.

12 How much each Party can be held responsible for

12.1 Each Party's total aggregate liability under this Assignment and Licence (whether in tort, contract or otherwise) for each claim or series of connected claims is no more than £1 million.

12.2 No Party is liable to the other for:

12.2.1 any indirect Losses; or

12.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

12.3 The limitation of liability set out in clause 11.1 does not apply to either Party in relation to the following:

12.3.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or subcontractors;

12.3.2 bribery or fraud or fraudulent misrepresentation by it or its employees; or

12.3.3 any liability that cannot be excluded or permitted by Law.

12.4 Each Party must use all reasonable endeavours to mitigate any Losses which it suffers under or in connection with this Assignment and Licence, including where any such Losses are covered by an indemnity.

12.5 When calculating the Supplier's liability under clause 11.1, Losses covered by Required Insurances will not be taken into consideration.

13 Invalid parts of this Assignment and Licence

13.1 If any part of this Assignment and Licence is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be removed from this Assignment and Licence as much as required and rendered ineffective as far as possible without affecting the rest of the Assignment and Licence, or whether it is valid or enforceable.

14 No other terms apply

14.1 Except as otherwise expressly provided in this Assignment and Licence or in the TQ Agreement, the provisions incorporated into this Assignment and Licence are the entire agreement between the Parties. The Assignment and Licence replaces all previous statements and agreements whether written or oral. No other provisions apply.

14.2 Variation of this Assignment and Licence is only effective if agreed in writing and signed by both Parties.

15 Other people's rights in this Assignment and Licence

15.1 No third parties may use the Contracts (Rights of Third Parties) Act ("**CRTPA**") to enforce any term of this Assignment and Licence unless stated (referring to CRTPA) in this Assignment and Licence. This does not affect third party rights and remedies that exist independently from CRTPA.

16 Relationships created by this Assignment and Licence

16.1 This Assignment and Licence does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

17 Giving up contract rights

17.1 A partial or full waiver or relaxation of the terms of this Assignment and Licence is only valid if it is stated to be a waiver in writing to the other Party.

18 Transferring responsibilities

18.1 The Supplier must not assign this Assignment and Licence without Approval.

18.2 The Authority can assign, novate or transfer this Assignment and Licence or any part of it to any Crown Body, public or private sector body which performs the functions of the Authority.

18.3 The Supplier must enter into a novation agreement in the form that the Authority specifies in order to use its rights under clause 17.2.

18.4 The Supplier can terminate this Assignment and Licence if it is novated under clause 17.2 to a private sector body that is experiencing an Insolvency Event.

19 How to communicate about this Assignment and Licence

19.1 All notices under this Assignment and Licence must be in writing and are considered effective on the Working Day of delivery as long as delivered before 5:00 pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

19.2 Notices to the Authority must be sent to the Authority Authorised Representative's address and email address, and all notices must be copied to the Authority's Head of Commercial Delivery Management [redacted] and the Authority's Head of Legal [redacted]

19.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

20 Dealing with claims

20.1 If a Beneficiary is notified or otherwise becomes aware of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days after such notification or date of first awareness.

20.2 At the Indemnifier's cost the Beneficiary must both:

20.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and

20.2.2 give the Indemnifier reasonable assistance with the Claim if requested.

20.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

20.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary's reputation.

20.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

20.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

20.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

20.7.1 the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or

20.7.2 the amount the Indemnifier paid the Beneficiary for the Claim.

21 Resolving disputes

21.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

21.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using clauses 20.3 to 20.5.

21.3 Unless the Authority refers the Dispute to arbitration using clause 20.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

21.3.1 determine the Dispute;

21.3.2 grant interim remedies, or any other provisional or protective relief.

21.4 The Supplier agrees that the Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

21.5 The Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 20.4, unless the Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 20.4.

21.6 The Supplier cannot suspend the performance of this Assignment and Licence during any Dispute.

22 Which law applies

22.1 This Assignment and Licence and any issues arising out of, or connected to it, are governed by English law.

ANNEX

IPR Assurance Certificate

This certificate is given pursuant to clause 13.9 of the agreement ("**Contract**") between the Institute for Apprenticeships and Technical Education ("**Authority**") and the supplier named below ("**Supplier**"), and the Intellectual Property Assignment and Licence between the Authority and the Supplier (which also forms Schedule 14 of the Contract) ("**Assignment and Licence**").

Guidance:

When to complete this certificate: This certificate should be completed in respect of each Deliverable (as defined in the Contract) which is made available to the Authority under the Contract, and a completed certificate should be supplied to the Authority with that Deliverable. This includes updates to existing Deliverables.

Purpose of this certificate: This certificate is intended to confirm that the specific Deliverable fully complies with the intellectual property provisions of the Contract. A copy of the certificate will be retained by the Authority as evidence of the intellectual property position.

Supplier Declaration:

We (being the Supplier named below) confirm that the Deliverable(s) supplied together with (or shortly before or after) this certificate, all elements of which are listed in either Table 1 or Table 2 below[4], comply with the intellectual property provisions in the Contract, in particular the applicable warranties set out in clause 5 of the Assignment and Licence.

We confirm that the Deliverable(s) either:
(i) contain no third party intellectual property rights, or
(ii) contain third party intellectual property rights and we have obtained the consent of the applicable third party:
- in the case of Key Materials, to their assignment and transfer to the Authority; and/or
- in the case of Ancillary Materials, to their licence to the Authority,

in each case on the terms and conditions of the Contract and Assignment and Licence.

We confirm that this certificate overrides any statement or copyright notice forming part of the Deliverable(s) which is in any way inconsistent with this certificate. We agree that this certificate does not detract in any way from the rights granted to the Authority in the Contract.

Key Materials

We confirm that the Deliverable(s) set out in Table 1 below, or the elements of the Deliverable(s) set out in Table 1 below, are Key Materials, as defined in the Contract:

[4] If, by exception, the Supplier asserts that the Deliverable includes elements which are neither Key Materials nor Ancillary Materials, this should be notified in writing to the Authority prior to the relevant Deliverable being made available to the Authority.

Table 1

Deliverable	Key Materials
[Set out title / description of the Deliverable]	Set out elements which are Key Materials, or confirm "entire Deliverable"
[insert additional rows if required]	

All intellectual property rights in the Deliverable(s), or elements of the Deliverable(s) listed above in Table 1 as Key Materials, have vested or hereby vest in the Authority pursuant to the Assignment and Licence.

Ancillary Materials

We confirm that the Deliverable(s) set out in Table 2 below, or the elements of the Deliverable set out in Table 2 below are Ancillary Materials, as defined in the Contract:

Table 2

Deliverable	Ancillary Materials
[Set out title / description of the Deliverable]	Set out elements which are Ancillary Materials, or confirm "entire Deliverable"
[insert additional rows if required]	

All intellectual property rights in the Deliverable(s), or elements of the Deliverable(s) listed above in Table 2 as Ancillary Materials, are licensed to the Authority on the terms and conditions of and pursuant to the Assignment and Licence.

Signed for and on behalf of the Supplier:

Name

Position

Date

Signed by

Pearson Education Limited

[redacted]

[redacted]

Signed by

THE INSTITUTE FOR APPRENTICESHIPS AND TECHNICAL EDUCATION

[redacted]

[redacted]