

SCHEDULE 1

DEFINITIONS

Schedule 1 (*Definitions*)

1 DEFINITIONS

- 1.1 In the Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Schedule 1 (*Definitions*) 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/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In the 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 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
 - 1.3.5 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";
 - 1.3.6 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;
 - 1.3.7 references to "representations" shall be construed as references to present facts, to "warranties" as references to present and future facts and to "undertakings" as references to obligations under the Contract;
 - 1.3.8 references to "Clauses" and "Schedules" are, unless otherwise provided, references to the clauses and schedules of 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;

Schedule 1 (Definitions)

- 1.3.9 references to "Paragraphs" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and
- 1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified.
- 1.3.11 the headings in the Contract are for ease of reference only and shall not affect the interpretation or construction of the Contract; and
- 1.3.12 where the Buyer is a Crown Body it shall be treated as contracting with the Crown as a whole.
- 1.4 Any reference in this Contract which immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to Section 1A of the European Union (Withdrawal) Act 2018) is a reference to (as it has effect from time to time):
- 1.4.1 any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("EU References") which is to form part of domestic law by application of Section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
- 1.4.2 any EU institution or EU authority or other such EU body shall be read on and after IP Completion Day as a reference to the UK institution, authority or body to which its functions were transferred.
- 1.5 Where a standard, policy or document is referred to in this Contract by reference to a hyperlink, then if the hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Authority and the Parties shall update this Contract with a reference to the replacement hyperlink.

"Accounting Reference Date" means in each year the date to which the Supplier prepares its annual audited financial statements;

"Achieve" (a) in respect of a Test, to successfully pass a Test without any Test Issues; and

(b) in respect of a Milestone, the issue of a Milestone Achievement Certificate in respect of that Milestone in accordance with the provisions of Schedule 14 (*Testing Procedures*),

and **"Achieved"** and **"Achievement"** shall be construed accordingly;

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

“Affiliate”	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 with, that body corporate from time to time;
“Annual Contract Report”	has the meaning given in Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Annual Revenue”	<p>means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:</p> <ul style="list-style-type: none">(a) figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and(b) where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
“Approved Sub-Licensee”	<p>any of the following:</p> <ul style="list-style-type: none">(a) a Central Government Body;(b) any third party providing services to a Central Government Body; and/or(c) any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Authority;
“Assets”	all assets and rights used by the Supplier to provide the Services in accordance with this Contract but excluding the Authority Assets;
“Associated Person”	has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017;
“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be

	treated as an associate under generally accepted accounting principles;
“Assurance”	means written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority;
“ATP Milestone”	the Milestone linked to Authority to Proceed for the relevant Operational Services set out in the Implementation Plan;
“Audit”	any exercise by the Authority of its Audit Rights pursuant to Clause 12 (Records, Reports, Audit and Open Book Data) and Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Audit Agents”	<ul style="list-style-type: none">(a) the Authority’s internal and external auditors;(b) the Authority’s statutory or regulatory auditors;(c) the Comptroller and Auditor General, their 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;
“Audit Rights”	the audit and access rights referred to in Part C of Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Authority Assets”	the Authority Materials, the Authority infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority and which is or may be used in connection with the provision or receipt of the Services;
“Authority Background IPRs”	<ul style="list-style-type: none">(a) IPRs owned by the Authority before the Effective Date, including IPRs contained in any of the Authority's Know-How, documentation, processes and procedures;(b) IPRs created by the Authority independently of this Contract; and/or(c) Crown Copyright which is not available to the Supplier otherwise than under this Contract;

but excluding IPRs owned by the Authority subsisting in the Authority Software;

“Authority Cause”

any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is:

- (a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or
- (b) caused by the Supplier, any Sub-contractor or any Supplier Personnel;

“Authority Data”

(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, and which are:

- (i) supplied to the Supplier by or on behalf of the Authority; and/or
- (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or

(b) any Personal Data for which the Authority is the Controller;

“Authority IT Strategy”

the Authority's IT policy in force as at the Effective Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Change Control Procedure;

“Authority Materials”

the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority to the Supplier, the IPRs in which:

- (a) are owned or used by or on behalf of the Authority; and
- (b) are or may be used in connection with the provision or receipt of the Services,

but excluding any Project Specific IPRs, Specially Written Software, Supplier Software, Third Party Software and Documentation relating to Supplier Software or Third Party Software;

Schedule 1 (Definitions)

“Authority Premises”	premises owned, controlled or occupied by the Authority and/or any Central Government Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them);
“Authority Representative”	the representative appointed by the Authority pursuant to Clause 11.4 (Representatives);
“Authority Requirements”	the requirements of the Authority set out in Schedule 2 (<i>Services Description</i>), Schedule 3 (<i>Performance Levels</i>), Schedule 4, Schedule 5 (<i>Security Management</i>), Schedule 6 (<i>Insurance Requirements</i>), Schedule 13 (<i>Implementation Plan</i>), Schedule 24 (<i>Reports and Records Provisions</i>), Schedule 25 (<i>Exit Management</i>) and Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Authority Responsibilities”	the responsibilities of the Authority specified in Schedule 7 (<i>Authority Responsibilities</i>);
“Authority Software”	software which is owned by or licensed to the Authority (other than under or pursuant to this Contract) and which is or will be used by the Supplier for the purposes of providing the Services;
“Authority System”	the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Supplier in connection with this Contract which is owned by the Authority or licensed to it by a third party and which interfaces with the Supplier System or which is necessary for the Authority to receive the Services;
“Authority to Proceed” or “ATP”	the authorisation to the Supplier to commence the provision of the relevant Operational Services to the Authority, provided by the Authority in the form of a Milestone Achievement Certificate in respect of the ATP Milestone;
“Balanced Scorecard Report”	has the meaning given in Paragraph 1.1(b) of Part B of Schedule 3 (<i>Performance Levels</i>);
“Board”	means the Supplier's board of directors;

“Board Confirmation”	means the written confirmation from the Board in accordance with Paragraph 8 of Schedule 18 (<i>Financial Distress</i>);
“Breakage Costs Payment”	has the meaning given in Schedule 16 (<i>Payments on Termination</i>);
“Cabinet Office Markets and Suppliers Team”	means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
“Central Government Body”	<p>a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <ul style="list-style-type: none">(a) Government Department;(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);(c) Non-Ministerial Department; or(d) Executive Agency;
“Certificate of Costs”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Change”	any change to this Contract;
“Change Authorisation Note”	a form setting out an agreed Contract Change which shall be substantially in the form of Annex 2: Change Authorisation Note;
“Change Control Procedure”	the procedure for changing this Contract set out in Schedule 22 (<i>Change Control Procedure</i>);
“Change in Law”	any change in Law which impacts on the performance of the Services which comes into force after the Effective Date;
“Change Request”	a written request for a Contract Change substantially in the form of Annex 1 (<i>Change Request Form</i>);
“Charges”	the charges for the provision of the Services set out in or otherwise calculated in accordance with

	Schedule 15 (<i>Charges and Invoicing</i>), including any Milestone Payment or Service Charge;
“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“CNI”	means Critical National Infrastructure;
“Commercially Sensitive Information”	<p>the information of a commercially sensitive nature relating to:</p> <ul style="list-style-type: none">(a) the pricing of the Services;(b) details of the Supplier’s IPRs; and(c) the Supplier’s business and investment plans; <p>which the Supplier has notified to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;</p>
“Comparable Supply”	the supply of services to another customer of the Supplier that are the same or similar to any of the Services;
“Computing Hubs”	means a school or college with expertise in computing that provides local-level engagement and support to other schools, and such hubs are identified in Annex 1 of Schedule 33 (Grant Funding and Incentive Payments) as at the Start Date;
“Confidential Information”	<ul style="list-style-type: none">(a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Contract that relates to:<ul style="list-style-type: none">(i) the Disclosing Party Group; or(ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Disclosing Party Group;(b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Contract that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient’s attention or into the

Recipient's possession in connection with this Contract;

(c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Contract and all matters arising therefrom; and

(d) Information derived from any of the above,

but not including any Information which:

(i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;

(ii) the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;

(iii) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Contract or breach of a duty of confidentiality;

(iv) was independently developed without access to the Confidential Information; or

(v) relates to the Supplier's:

(1) performance under this Contract; or

(2) failure to pay any Sub-contractor as required pursuant to Clause 15.15(a) (Supply Chain Protection);

"Conflict of Interest"

a conflict between the financial or personal duties of the Supplier or the Supplier Personnel and the duties owed to the Authority under the Contract, in the reasonable opinion of the Authority;

"Contract Change"

any change to this Contract other than an Operational Change;

“Contract Inception Report”	the initial financial model in a form agreed by the Supplier and the Authority in writing on or before the Effective Date;
“Contracts Finder”	the online government portal which allows suppliers to search for information about contracts as prescribed by Part 4 of the Public Contract Regulations 2015;
“Contract Year”	<p>(a) a period of 12 months commencing on the Operational Services Commencement Date; or</p> <p>(b) thereafter a period of 12 months commencing on each anniversary of the Operational Services commencement Date;</p> <p>provided that the final Contract Year shall end on the expiry or termination of the Term;</p>
“Control”	the possession by person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Controller”	has the meaning given in the UK GDPR or the EU GDPR as the context requires;
“Corporate Change Event”	<p>means:</p> <p>(a) any change of Control of the Supplier or a Parent Undertaking of the Supplier;</p> <p>(b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services;</p> <p>(c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services;</p> <p>(d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;</p>

- (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;
- (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;
- (g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;
- (h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;
- (i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or
- (j) any process or events with an effect analogous to those in Paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;

“Corporate Change Event Grace Period”

means a grace period agreed to by the Relevant Authority for providing CRP Information and/or updates to Service Continuity Plan after a Corporate Change Event

“Corporate Resolvability Assessment (Structural Review)”

means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 and Annex 2: Corporate Resolvability Assessment (Structural Review) of Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);

“CPP Milestone”

a contract performance point as set out in the Implementation Plan, being the Milestone at which the Supplier has demonstrated that the Supplier

	Solution or relevant Service is working satisfactorily in its operating environment in accordance with Schedule 14 (<i>Testing Procedures</i>);
“Critical National Infrastructure”	<p>means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>(a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>(b) significant impact on the national security, national defence, or the functioning of the UK;</p>
“Critical Service Contract”	means the overall status of the Services provided under this Contract as determined by the Authority and specified in Paragraph 1.1 of Part B to Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Crown Body”	means the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
“Crown Copyright”	has the meaning given in the Copyright, Designs and Patents Act 1988
“CRP Information”	<p>means the Corporate Resolution Planning Information, together, the:</p> <p>(a) Exposure Information (Contracts List);</p> <p>(b) Corporate Resolvability Assessment (Structural Review); and</p> <p>(c) Financial Information and Commentary</p>
“CRTPA”	the Contracts (Rights of Third Parties) Act 1999;

“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	an assessment by the Controller carried out in accordance with section 3 o Chapter IV of the UK GDPR and sections 64 and 65 of the DPA 2018;
“Data Protection Legislation”	(c) (i) all applicable UK law relating to the processing of personal data and privacy, including but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and (ii) (to the extent that it may be applicable) the EU GDPR). The UK GDPR and EU GDPR are defined in section 3 of the Data Protection Act 2018.;
“Data Subject”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Data Subject Request”	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to their Personal Data;
“Deductions”	all Service Credits, or any other deduction which is paid or payable to the Authority under this Contract;
“Default”	<p>any breach of the obligations of the relevant Party (including abandonment of this Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement:</p> <p>(a) in the case of the Authority, of its employees, servants, agents; or</p> <p>(b) in the case of the Supplier, of its Sub-contractors or any Supplier Personnel,</p> <p>in connection with or in relation to the subject-matter of this Contract and in respect of which such Party is liable to the other;</p>
“Defect”	(a) any error, damage or defect in the manufacturing of a Deliverable; or

	<ul style="list-style-type: none">(b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or(c) any failure of any Deliverable to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; or(d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria;
“Delay”	<ul style="list-style-type: none">(a) a delay in the Achievement of a Milestone by its Milestone Date; or(b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
“Delay Deduction Period”	the period of one hundred (100) days commencing on the relevant Milestone Date;
“Delay Payments”	the amounts payable by the Supplier to the Authority in respect of a Delay in Achieving a Key Milestone as specified in Schedule 15 (<i>Charges and Invoicing</i>);
“Deliverable”	an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Contract;
“Dependent Parent Undertaking”	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Contract, including for the

	avoidance of doubt the provision of the Services in accordance with the terms of this Contract;
“Detailed Implementation Plan”	the plan developed and revised from time to time in accordance with Paragraphs 3 and 4 of Schedule 13 (<i>Implementation Plan</i>);
“Disclosing Party”	has the meaning given in Clause 19.1 (Confidentiality);
“Disclosing Party Group”	(a) where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and (b) where the Disclosing Party is the Authority, the Authority and any Central Government Body with which the Authority or the Supplier interacts in connection with this Contract;
“Dispute”	any dispute, difference or question of interpretation arising out of or in connection with this Contract, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Change Control Procedure or any matter where this Contract directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure;
“Dispute Notice”	a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute;
“Dispute Resolution Procedure”	the dispute resolution procedure set out in Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Documentation”	descriptions of the Services and Performance Indicators, details of the Supplier System (including (i) vendors and versions for off-the-shelf components and (ii) source code and build information for proprietary components), relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as: (a) is required to be supplied by the Supplier to the Authority under this Contract;

	<ul style="list-style-type: none">(b) 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 provide Services;(c) is required by the Supplier in order to provide the Services; and/or(d) has been or shall be generated for the purpose of providing the Services;
“DOTAS”	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to national insurance contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
“DPA 2018”	the Data Protection Act 2018;
“Due Diligence Information”	any information supplied to the Supplier by or on behalf of the Authority prior to the Effective Date;
“Effective Date”	<ul style="list-style-type: none">(a) the date on which this Contract is signed by both Parties;(b)
“EIRs”	the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Central Government Body in relation to such Regulations;
“Emergency Maintenance”	<p>ad hoc and unplanned maintenance provided by the Supplier where:</p> <ul style="list-style-type: none">(a) the Authority reasonably suspects that the IT Environment or the Services, or any part of the IT Environment or the Services, has or may

have developed a fault, and notifies the Supplier of the same; or

- (b) the Supplier reasonably suspects that the IT Environment or the Services, or any part the IT Environment or the Services, has or may have developed a fault;

“Employee Liabilities”

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 related to employment including in relation to the following:

- (a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;
- (b) unfair, wrongful or constructive dismissal compensation;
- (c) 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;
- (d) compensation for less favourable treatment of part-time workers or fixed term employees;
- (e) outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions;
- (f) employment claims whether in tort, contract or statute or otherwise;
- (g) any investigation relating to employment matters 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;

“Employment Regulations”

the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced;

“EEA”	European Economic Area
“EU GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
“EU”	European Union
“Exit Management”	services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Authority and/or a Replacement Supplier, as set out or referred to in Schedule 25 (<i>Exit Management</i>);
“Exit Plan”	the plan produced and updated by the Supplier during the Term in accordance with Paragraph 5 of Schedule 25 (<i>Exit Management</i>);
“Expedited Dispute Timetable”	the reduced timetable for the resolution of Disputes set out in Paragraph 3 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Expert”	has the meaning given in Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Expert Determination”	the process described in Paragraph 6 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Exposure Information (Contracts List)”	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 and Annex 1 of Part B of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Extension Period”	a period of 12 months from the end of the Initial Term;
“Financial Distress Event”	the occurrence of one or more of the events listed in Paragraph 3.1 of Schedule 18 (<i>Financial Distress</i>);
“Financial Information and Commentary”	means part of the CRP Information requirements set out in accordance with Paragraphs 2 and Annex 3 of Part B of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);

Schedule 1 (Definitions)

“Financial Distress Remediation Plan”	a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Contract in the event that a Financial Distress Event occurs. This plan should include what the Authority would need to put in place to ensure performance and delivery of the Services in accordance with this Contract up to and including any Insolvency Event in respect of the relevant FDE Group entity and may refer to the Insolvency Continuity Plan in this regard;
“Financial Reports”	has the meaning given in Schedule 19 (<i>Financial Reports and Audit Rights</i>);
“Financial Transparency Objectives”	has the meaning given in Schedule 19 (Financial Reports and Audit Rights);
“FOIA”	the Freedom of Information Act 2000 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 any relevant Central Government Body in relation to such Act;
“Force Majeure Event”	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 riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or other natural disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier’s or a Sub-contractor’s supply chain;
“Force Majeure Notice”	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”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);

“General Anti-Abuse Rule”	<p>(a) the legislation in Part 5 of the Finance Act 2013; and</p> <p>(b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions;</p>
“General Change in Law”	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 affects or relates to a Comparable Supply;
“Good Industry Practice”	at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Authority, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws;
“Grant Administrator”	means the Supplier in its role as administrator of the Grant Funding;
“Grant Funding”	<p>means funding payments made to Computing Hubs through the Supplier in accordance with Grant Funding Terms and Conditions for the purposes of:</p> <ul style="list-style-type: none">• contributing to salaries to ensure each Computing Hub has sufficient resource allocated;• delivery of CPD to teachers;• running reach and engagement activities for schools; and• supporting schools more generally to improve their computing education provision;
“Grant Funding Terms and Conditions”	the terms and conditions to be entered into between the Supplier and Computing Hubs for the payment of Grant Funding similar to the form set out in Annex 2 of the Schedule 33 (Grant Funding and Incentive Payments);
“Grant Offer Letter”	means the offer letter, to be sent to Computing Hubs who have been granted Grant Funding which shall

	be issued to the Supplier by the Authority following the Effective Date;
“Halifax Abuse Principle”	the principle explained in the CJEU Case C-255/02 Halifax and others;
“Health and Safety Policy”	the health and safety policy of the Authority and/or other relevant Central Government Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety;
“HMRC”	HM Revenue & Customs;
“Impact Assessment”	has the meaning given in Schedule 22 (<i>Change Control Procedure</i>);
“Implementation Milestones”	the Milestones related to Implementation which upon Achievement of such by the Milestone Date will result in the Authority paying the Supplier the Implementation Milestone Payments as set out in Annex 1 of Schedule 15 (Charges and Invoicing);
“Implementation Milestone Payments”	the payments set out in Annex 1 of Schedule 15 (Charges and Invoicing) to be made to the Supplier upon Achieving the relevant Implementation Milestone;
“Implementation Plan”	the Outline Implementation Plan or (if and when approved by the Authority pursuant to Paragraph 3 of Schedule 13 (<i>Implementation Plan</i>)) the Detailed Implementation Plan as updated in accordance with Paragraph 4 of Schedule 13 (<i>Implementation Plan</i>) from time to time;
“Implementation Services”	the implementation services described as such in the Services Description;
“Implementation Services Commencement Date”	the date on which the Supplier is to commence provision of the first of the Services, being the Effective Date;
“Incentive Payments”	the payments made by the Supplier to schools for the activities set out in Paragraphs 2.2.2 and 2.2.3

	of Schedule 33 (Grant Funding and Incentive Payments);
“Indemnified Person”	the Authority and each and every person to whom the Authority (or any direct or indirect sub-licensee of the Authority) sub-licenses, assigns or novates any Relevant IPRs or rights in Relevant IPRs in accordance with this Contract;
“Independent Controller”	a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data;
“Information”	all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form);
“Initial Term”	the period from and including the Effective Date to 31 st August 2025;
“Initial Upload Date”	means the occurrence of an event detailed in Schedule 24 (<i>Reports and Records Provisions</i>) Annex 3: (<i>Records To Upload To Virtual Library</i>) which requires the Supplier to provide its initial upload of the relevant information to the Virtual Library;
“Insolvency Event”	<p>with respect to any person, means:</p> <ul style="list-style-type: none">(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:<ul style="list-style-type: none">(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more

of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

- (c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;
- (d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within fourteen (14) days;
- (e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;
- (f) where that person is a company, a LLP or a partnership:
 - (i) a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;
 - (ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;
 - (iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or

- (iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or
 - (g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;
- “Intellectual Property Rights” or “IPRs”**
- (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 names, 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;
- “Intervention Cause”**
- has the meaning given in Clause 27.1 (Remedial Adviser);
- “Intervention Notice”**
- has the meaning given in Clause 27.1 (Remedial Adviser);
- “Intervention Period”**
- has the meaning given in Clause 27.2(c) (Remedial Adviser);
- “Intervention Trigger Event”**
- (a) any event falling within limb (a), (b), (c), (f) or (g) of the definition of a Supplier Termination Event;
 - (b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services;
 - (c) the Supplier not Achieving a Milestone within seventy-five (75) days of its relevant Milestone Date;

“IP Completion Day”	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;
“IPRs Claim”	any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs save for any such claim to the extent that it is caused by any use by or on behalf of that Indemnified Person of any Relevant IPRs, or the use of the Authority Software by or on behalf of the Supplier, in either case in combination with any item not supplied or recommended by the Supplier pursuant to this Contract or for a purpose not reasonably to be inferred from the Services Description or the provisions of this Contract;
“IT”	information and communications technology;
“IT Environment”	the Authority System and the Supplier System;
“Joint Controllers”	where two or more Controllers jointly determine the purposes and means of processing;
“Key Milestone”	the key milestones as detailed in Annex 1 of Schedule 15 (Charges and Invoicing) and in respect of which Delay Payments may be payable in accordance with Paragraph 1 of Part C of Schedule 15 (Charges and Invoicing) if the Supplier fails to Achieve the Milestone Date in respect of such Milestone;
“Key Performance Indicator”	the key performance indicators set out in Table 1 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Key Personnel”	those persons appointed by the Supplier to fulfil the Key Roles, being the persons listed in Schedule 29 (<i>Key Personnel</i>) against each Key Role as at the Effective Date or as amended from time to time in accordance with Clauses 14.5 and 14.6 (Key Personnel);
“Key Roles”	a role described as a Key Role in Schedule 29 (<i>Key Personnel</i>) and any additional roles added from time to time in accordance with Clause 14.4 (Key Personnel);

“Key Sub-contract”	each Sub-contract with a Key Sub-contractor;
“Key Sub-contractor”	any Sub-contractor: <ul style="list-style-type: none">(a) 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; and/or(b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under this Contract (as set out in the Financial Model);
“Know-How”	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Services but excluding know how already in the other Party’s possession before this Contract;
“KPI Failure”	a failure to meet the Target Performance Level in respect of a Key Performance Indicator;
“KPI Milestone”	the Milestones which upon Achievement of such by the Milestone Date will result in the Authority paying the Supplier the KPI Milestone Payments as set out in Annex 1 of Schedule 15 (Charges and Invoicing);
“KPI Milestone Payment”	the payments set out in Annex 1 of Schedule 15 (Charges and Invoicing) to be made to the Supplier upon Achieving the relevant KPI Milestone in accordance with the KPI Milestone Payment threshold for the relevant KPIs set out in Table 1 Part A of Annex 1 of Schedule 3 (Performance Levels);
“Law”	any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;

Schedule 1 (Definitions)

“LED”	Law Enforcement Directive (Directive (EU) 2016/680);
“Licensed Software”	all and any Software licensed by or through the Supplier, its Sub-contractors or any third party to the Authority for the purposes of or pursuant to this Contract, including any Supplier Software, Third Party Software and/or any Specially Written Software;
“Losses”	losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
“Maintenance Schedule”	shall have the meaning set out in Clause 9.4 (Maintenance);
“Malicious Software”	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
“Management Information”	the management information specified in Schedule 3 (<i>Performance Levels</i>), Schedule 15 (<i>Charges and Invoicing</i>) and Schedule 21 (<i>Governance</i>) to be provided by the Supplier to the Authority;
“Measurement Period”	in relation to a Key Performance Indicator or Subsidiary Performance Indicator, the period over which the Supplier’s performance is measured (for example, a Service Period if measured monthly or a 12 month period if measured annually);
“Milestone”	an event or task described in the Implementation Plan which, if applicable, shall be completed by the relevant Milestone Date;
“Milestone Achievement Certificate”	the certificate to be granted by the Authority when the Supplier has Achieved a Milestone, which shall be in substantially the same form as that set out in Annex 3 of Schedule 14 (<i>Testing Procedures</i>);

“Milestone Date”	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
“Milestone Payment”	a payment identified in Schedule 15 (<i>Charges and Invoicing</i>) to be made following the issue of a Milestone Achievement Certificate;
“Milestone Retention”	has the meaning given in Schedule 15 (<i>Charges and Invoicing</i>);
“Modern Slavery Assessment Tool”	means the modern slavery risk identification and management tool which can be found online at: https://supplierregistration.cabinetoffice.gov.uk/msat/]
“month”	a calendar month and “monthly” shall be interpreted accordingly;
“Multi-Party Dispute Resolution Procedure”	has the meaning given in Paragraph 9.1 of Schedule 28 (<i>Staff Transfer</i>) of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“Multi-Party Procedure Initiation Notice”	has the meaning given in Paragraph 9.2 of Schedule 23 (<i>Dispute Resolution Procedure</i>);
“NCSC”	the National Cyber Security Centre or any replacement or successor body carrying out the same function;
“New Releases”	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
“Non-trivial Customer Base”	a significant customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor;
“Notifiable Default”	shall have the meaning given in Clause 25.1 (Rectification Plan Process);
“Object Code”	software and/or data in machine-readable, compiled object code form;

“Occasion of Tax Non-Compliance”

- (a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of:
 - (i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;
 - (ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or
- (b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise on or after 1 April 2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a civil penalty for fraud or evasion;

“Open Book Data”

has the meaning given in Schedule 19 (*Financial Reports and Audit Rights*);

“Open Source”

computer Software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source;

“Operating Environment”

the Authority System and the Sites;

“Operational Change”

any change in the Supplier's operational procedures which in all respects, when implemented:

- (a) will not affect the Charges and will not result in any other costs to the Authority;
- (b) may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services;

	(c) will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure; and
	(d) will not require a change to this Contract;
“Operational Service Commencement Date”	means 1 st April 2023;;
“Operational Services”	the operational services described as such in the Services Description;
“Other Supplier”	any supplier to the Authority (other than the Supplier) which is notified to the Supplier from time to time;
“Outline Implementation Plan”	the outline plan set out at Annex 1 of Schedule 13 (<i>Implementation Plan</i>);
“Parent Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Partial Termination”	the partial termination of this Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 31.2(b) (Termination by the Authority) or 31.3(b) (Termination by the Supplier) or otherwise by mutual agreement by the Parties;
“Parties” and “Party”	have the meanings respectively given on page 1 of this Contract;
“Performance Failure”	a KPI Failure or a PI Failure;
“Performance Indicators”	the Key Performance Indicators and the Subsidiary Performance Indicators;
“Permitted Maintenance”	has the meaning given in Clause 9.4 (Maintenance);
“Performance Monitoring Report”	has the meaning given in Schedule 3 (<i>Performance Levels</i>);
“Personal Data”	has the meaning given in the UK GDPR or the EU GDPR as the context requires;
“Personal Data Breach”	has the meaning given in the UK GDPR or the EU GDPR as the context requires;

“PI Failure”	a failure to meet the Target Performance Level in respect of a Subsidiary Performance Indicator;
“PI Service Threshold”	shall be as set out against the relevant Subsidiary Performance Indicator in Table 2 in Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Preceding Services”	has the meaning given in Clause 5.2(b) (Standard of Services);
“Prescribed Person”	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’, 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 , as updated from time to time;
“Processor”	has the meaning given to it under the UK GDPR or the EU GDPR as the context requires;
“Processor Personnel”	means all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Sub-processor engaged in the performance of its obligations under this Contract;
“Programme Board”	the body described in Paragraph 5 of Schedule 21 (<i>Governance</i>) known as the NCCE Steering Group;
“Prohibited Act”	<ul style="list-style-type: none">(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to:<ul style="list-style-type: none">(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;(c) an offence:

- (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act);
 - (ii) under legislation or common law concerning fraudulent acts; or
 - (iii) defrauding, attempting to defraud or conspiring to defraud the Authority (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); 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;

“Protective Measures” appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Contract, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it including those outlined in Schedule 5 (Security Management).;

“Project Specific IPRs” (a) Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Contract and updates and amendments of these items including (but not limited to) database schema; and/or

(b) Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under this Contract;

but shall not include the Supplier Background IPRs or the Specially Written Software;

“Public Sector Dependent Supplier” means a supplier where that supplier, or that supplier's group has Annual Revenue of [REDACTED] or more of which over 50% is generated from UK Public Sector Business;

“Publishable Performance Information”	means any of the information in the Performance Monitoring Report as it relates to a Performance Indicator where it is expressed as publishable in the table in Annex 1 which shall not constitute Commercially Sensitive Information;
“Quality Plans”	has the meaning given in Clause 6.1 (Quality Plans);
“Quarter”	the first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall end on the date of termination or expiry of this Contract);
“Recipient”	has the meaning given in Clause 19.1 (Confidentiality);
“Records”	has the meaning given in Schedule 24 (<i>Reports and Records Provisions</i>);
“Rectification Plan”	a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default Material KPI ;
“Rectification Plan Failure”	<ul style="list-style-type: none">(a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 25.4 (Submission of the draft Rectification Plan) or 25.8 (Agreement of the Rectification Plan);(b) the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 25.7 (Agreement of the Rectification Plan);(c) the Supplier failing to rectify a material Default within the later of:<ul style="list-style-type: none">(i) 30 Working Days of a notification made pursuant to Clause 25.2 (Notification); and(ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default;(d) a KPI Failure re-occurring in respect of the same Key Performance Indicator for the same (or substantially the same) root cause in any two consecutive Measurement Periods, the second

and any subsequent such KPI Failure shall be a Repeat KPI Failure

- (e) the Supplier not Achieving a Key Milestone by the expiry of the Delay Deduction Period; and/or
- (f) following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of 6 months for the same (or substantially the same) root cause as that of the original Notifiable Default;

“Rectification Plan Process”

the process set out in Clauses 25.4 (Submission of the draft Rectification Plan) to 25.9 (Agreement of the Rectification Plan);

“Registers”

has the meaning given in Schedule 25 (*Exit Management*);

“Reimbursable Expenses”

has the meaning given in Schedule 15 (*Charges and Invoicing*);

“Relevant Authority” or “Relevant Authorities”

means the Authority and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;

“Relevant IPRs”

IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier’s obligations under this Contract including IPRs in the Specially Written Software, the Supplier Non-COTS Software, the Supplier Non-COTS Background IPRs, the Third Party Non-COTS Software and the Third Party Non-COTS IPRs but excluding any IPRs in the Authority Software, the Authority Background IPRs, the Supplier COTS Software, the Supplier COTS Background IPRs, the Third Party COTS Software and/or the Third Party COTS IPRs;

“Relevant Preceding Services”

has the meaning given in Clause 5.2(b) (Standard of Services);

“Relevant Requirements”

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;

Schedule 1 (Definitions)

“Relevant Tax Authority”	HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established;
“Relevant Transfer”	a transfer of employment to which the Employment Regulations applies;
“Relief Notice”	has the meaning given in Clause 29.2 (Authority Cause);
“Remedial Adviser”	the person appointed pursuant to Clause 27.2 (Remedial Adviser);
“Remedial Adviser Failure”	has the meaning given in Clause 27.6 (Remedial Adviser);
“Repeat KPI Failure”	has the meaning given in Schedule 3 (Performance Levels) Paragraph 1.1 of Part A;
“Replacement Services”	any services 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”	any third party service provider of Replacement Services appointed by the Authority from time to time (or where the Authority is providing replacement Services for its own account, the Authority);
“Request For Information”	a Request for Information under the FOIA or the EIRs;
“Required Action”	has the meaning given in Clause 28.1(a) (Step-In Rights);
“Risk Register”	the register of risks and contingencies that have been factored into any Charges due under this Contract, a copy of which is set out in the Virtual Library;
“Security Management Plan”	the Supplier's security plan as attached as Annex 2 of <i>Schedule 5 (Security Management)</i> and as subsequently developed and revised pursuant to Paragraphs 3 and 4 of Schedule 5 (<i>Security Management</i>);

“Security Requirements”	the Authority’s security requirements, the current copy of which is contained in Annexures 1 and 2 of Schedule 5 (<i>Security Management</i>), as updated from time to time by the Authority and notified to the Supplier;
“Service Charges”	the periodic payments made in accordance with Schedule 15 (<i>Charges and Invoicing</i>) in respect of the supply of the Operational Services;
“Service Continuity Plan”	any plan prepared pursuant to Paragraph 2 of Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>) as may be amended from time to time;
“Service Continuity Services”	the business continuity, disaster recovery and insolvency continuity services set out in Schedule 26 (<i>Service Continuity Plan and Corporate Resolution Planning</i>);
“Service Credit Cap”	means Service Credits of [REDACTED] each rolling 12 month period from Operational Service Commencement Date;
“Service Credits”	credits payable by the Supplier due to the accrual of Service Points, calculated in accordance with Paragraph 3 of Part C of Schedule 15 (<i>Charges and Invoicing</i>);
“Service Period”	<p>a calendar month, save that:</p> <p>(a) the first service period shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; and</p> <p>(b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;</p>
“Service Points”	in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the fifth column of the table in Annex 1 of Schedule 3 (<i>Performance Levels</i>);

“Services”	any and all of the services to be provided by the Supplier under this Contract, including those set out in Schedule 2 (<i>Services Description</i>);
“Service Transfer Date”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Services Description”	the services description set out in Schedule 2 (<i>Services Description</i>);
“Sites”	<p>any premises (including the Authority Premises, the Supplier’s premises or third party premises):</p> <p>(a) from, to or at which:</p> <p>(i) the Services are (or are to be) provided; or</p> <p>(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or</p> <p>(b) where:</p> <p>(i) any part of the Supplier System is situated; or</p> <p>(ii) any physical interface with the Authority System takes place;</p>
“SME”	an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
“Social Value”	the additional social benefits that can be achieved in the delivery of the Contract, set out in the Authority’s Requirements;
“Social Value PI”	The Social Value performance indicators set out in Table 2 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Social Value KPI”	The Social Value key performance indicators set out in Table 1 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);
“Software”	Specially Written Software, Supplier Software and Third Party Software;

“Software Supporting Materials”	has the meaning given in Paragraph 2.1(b) of Schedule 32 (<i>Intellectual Property Rights</i>) (Specially Written Software and Project Specific IPRs);
“Source Code”	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
“Specially Written Software”	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to Supplier Software or Third Party Software created specifically for the purposes of this Contract.
“Specific Change in Law”	a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply;
“Staffing Information”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Standards”	the standards, policies and/or procedures identified in Schedule 4 (<i>Standards</i>);
“Step-In Notice”	has the meaning given in Clause 28.1 (Step-In Rights);
“Step-In Trigger Event”	<ul style="list-style-type: none">(a) any event falling within the definition of a Supplier Termination Event;(b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services;(c) the Authority considers that the circumstances constitute an emergency despite the Supplier not being in breach of its obligations under this Contract;

	<ul style="list-style-type: none">(d) the Authority being advised by a regulatory body that the exercise by the Authority of its rights under Clause 28 (Step-In Rights) is necessary;(e) the existence of a serious risk to the health or safety of persons, property or the environment in connection with the Services; and/or(f) a need by the Authority to take action to discharge a statutory duty;
“Step-Out Date”	has the meaning given in Clause 28.5(b) (Step-In Rights);
“Step-Out Notice”	has the meaning given in Clause 28.5 (Step-In Rights);
“Step-Out Plan”	has the meaning given in Clause 28.6 (Step-In Rights);
“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Sub-contract”	any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
“Sub-contractor”	<p>any third party with whom:</p> <ul style="list-style-type: none">(a) the Supplier enters into a Sub-contract; or(b) a third party under (a) above enters into a Sub-contract, <p>or the servants or agents of that third party;</p>
“Sub-processor”	any third party appointed to process Personal Data on behalf of the Processor related to this Contract;
“Subsidiary Performance Indicator”	the performance indicators set out in Table 2 of Part A of Annex 1 of Schedule 3 (<i>Performance Levels</i>);

Schedule 1 (Definitions)

“Subsidiary Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Successor Body”	has the meaning given in Clause 34.4 (Assignment and Novation);
“Supplier Background IPRs”	<p>(a) Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Supplier's Know-How or generic business methodologies; and/or</p> <p>(b) Intellectual Property Rights created by the Supplier independently of this Contract,</p> <p>which in each case is or will be used before or during the Term for designing, testing implementing or providing the Services but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software;</p>
“Supplier COTS Background IPRs”	<p>Any embodiments of Supplier Background IPRs that:</p> <p>(a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and</p> <p>(b) has a Non-trivial Customer Base;</p>
“Supplier COTS Software”	<p>Supplier Software (including open source software) that:</p> <p>(a) the Supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and</p> <p>(b) has a Non-trivial Customer Base;</p>
“Supplier Equipment”	the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased or loaned from the Authority) for the provision of the Services;

Schedule 1 (Definitions)

“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
“Supplier Non-COTS Background IPRs”	Any embodiments of Supplier Background IPRs that have been delivered by the Supplier to the Authority and that are not Supplier COTS Background IPRs;
“Supplier Non-COTS Software”	Supplier Software that is not Supplier COTS Software;
“Supplier Non-Performance”	has the meaning given in Clause 29.1 (Authority Cause);
“Supplier Personnel”	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-contractor engaged in the performance of the Supplier’s obligations under this Contract;
“Supplier Representative”	the representative appointed by the Supplier pursuant to Clause 11.3 (Representatives);
“Supplier Software”	software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 12 (<i>Software</i>);
“Supplier Solution”	the Supplier’s solution for the Services set out in Schedule 8 (<i>Supplier Solution</i>) including any Annexes of that Schedule;
“Supplier System”	the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);
“Supplier Termination Event”	<p>(a) the Supplier committing a material Default which is irremediable;</p> <p>(b) as a result of the Supplier’s Default, the Authority incurring Losses in any Contract Year which exceed 80% of the value of the aggregate annual liability cap for that Contract Year as set</p>

out in Clause 23.6(a) (Financial and other Limits);

- (c) a Remedial Adviser Failure;
 - (d) a Rectification Plan Failure;
 - (e) where a right of termination is expressly reserved in this Contract, including pursuant to:
 - (i) Clause 17 (IPRs Indemnity);
 - (ii) Clause 36 (Compliance)
 - (iii) Clause 37.6(b) (Prevention of Fraud and Bribery); and/or
 - (iv) Paragraph 6 of Schedule 18 (*Financial Distress*);
 - (v) Paragraph 3 of Part B to Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);
 - (f) the representation and warranty given by the Supplier pursuant to Clause 3.2(i) (Warranties) being materially untrue or misleading;
 - (g) the Supplier committing a material Default under Clause 10.10 (Promoting Tax Compliance) or failing to provide details of steps being taken and mitigating factors pursuant to Clause 10.10 (Promoting Tax Compliance) which in the reasonable opinion of the Authority are acceptable;
 - (h) the Supplier committing a material Default under any of the following Clauses:
 - (i) Clause 5.5(j) (Services);
 - (ii) Clause 21 (Protection of Personal Data);
 - (iii) Clause 20 (Transparency and Freedom of Information);
 - (iv) Clause 19 (Confidentiality); and
 - (v) Clause 33 (Compliance); and/or
- in respect of any security requirements set out in Schedule 2 (*Services Description*), Schedule 5 (*Security Management*) or the Security Requirements; and/or

in respect of any requirements set out in Schedule 28 (*Staff Transfer*);

- (i) an Insolvency Event occurring in respect of the Supplier;
- (j) a change of Control of the Supplier unless:
 - (i) the Authority has given its prior written consent 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;
- (k) a change of Control of a Key Sub-contractor unless, within 6 months of being notified by the Authority that it objects to such change of Control, the Supplier terminates the relevant Key Sub-contract and replaces it with a comparable Key Sub-contract which is approved by the Authority pursuant to Clause 15.10 (Appointment of Key Sub-contractors);
- (l) any failure by the Supplier to enter into or to comply with an Admission Agreement under the Annex to either Part A or Part B of Schedule 28 (*Staff Transfer*);
- (m) the Authority has become aware that the Supplier should have been excluded under Regulation 57(1) or (2) of the Public Contracts Regulations 2015 from the procurement procedure leading to the award of this Contract;
- (n) a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law; or
- (o) in relation to Schedule 5 (*Security Management*):
 - (i) the Authority has issued two rejection notices in respect of the Security Management Plan under Paragraph 4.5(b) ([Part A](#));

- (ii) the Supplier fails to implement a change required by the Required Changes Register in accordance with the timescales set out in the Required Changes Register;
- (iii) Supplier COTS Software and Third Party COTS Software is not within mainstream support unless the Authority has agreed in writing.
- (iv) the Supplier fails to patch vulnerabilities in accordance with the Security Requirements; and/or,
- (v) the Supplier fails to comply with the Incident Management Process.

“Supply Chain Map”	<p>means details of (i) the Supplier, (ii) all Subcontractors and (iii) any other entity that the Supplier is aware is in its supply chain that is not a Subcontractor, setting out at least:</p> <ul style="list-style-type: none">(a) the name, registered office and company registration number of each entity in the supply chain;(a) the function of each entity in the supply chain; and <p>the location of any premises at which an entity in the supply chain carries out a function in the supply chain;</p>
“Supply Chain Transparency Report”	<p>means the report provided by the Supplier to the Authority in the form set out in Annex 4 of Schedule 24 (<i>Reports and Records Provisions</i>);</p>
“Target Performance Level”	<p>the minimum level of performance for a Performance Indicator which is required by the Authority, as set out against the relevant Performance Indicator in the tables in Annex 1 of Schedule 3 (<i>Performance Levels</i>);</p>
“Term”	<p>the period commencing on the Effective Date and ending on the expiry of the Initial Term or any Extension Period or on earlier termination of this Contract;</p>
“Termination Assistance Notice”	<p>has the meaning given in Paragraph 5 of Schedule 25 (<i>Exit Management</i>);</p>

“Termination Assistance Period”	in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services as such period may be extended pursuant to Paragraph 5.2 of Schedule 25 (<i>Exit Management</i>);
“Termination Date”	the date set out in a Termination Notice on which this Contract (or a part of it as the case may be) is to terminate;
“Termination Notice”	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 (or any part thereof) on a specified date and setting out the grounds for termination;
“Termination Payment”	the payment determined in accordance with Schedule 16 (<i>Payments on Termination</i>);
“Termination Services”	the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Annex 1 of Schedule 25 (<i>Exit Management</i>), and any other services required pursuant to the Termination Assistance Notice;
“Test Issues”	has the meaning given in Schedule 14 (<i>Testing Procedures</i>);
“Tests” and “Testing”	any tests required to be carried out under this Contract, as further described in Schedule 14 (<i>Testing Procedures</i>) and “Tested” shall be construed accordingly;
“Test Success Criteria”	has the meaning given in Schedule 14 (<i>Testing Procedures</i>);
“Third Party Auditor”	an independent third party auditor as appointed by the Authority from time to time to confirm the completeness and accuracy of information uploaded to the Virtual Library in accordance with the requirements outlined in Schedule 24 (<i>Reports and Records Provisions</i>);
“Third Party Beneficiary”	has the meaning given in Clause 41.1 (Third Party Rights);

“Third Party COTS IPRs”	Third Party IPRs that: <ul style="list-style-type: none">(a) the supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and(b) has a Non-trivial Customer Base;
“Third Party COTS Software”	Third Party Software (including open source software) that: <ul style="list-style-type: none">(a) the supplier makes generally available commercially prior to the date of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and(b) has a Non-trivial Customer base;
“Third Party IPRs”	Intellectual Property Rights owned by a third party, but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software, which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services;
“Third Party Non-COTS IPRs”	Third Party IPRs that are not Third Party COTS IPRs;
“Third Party Non-COTS Software”	Third Party Software that is not Third Party COTS Software;
“Third Party Provisions”	has the meaning given in Clause 41.1 (Third Party Rights);
“Third Party Software”	software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source Software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 12 (<i>Software</i>);
“Transferring Assets”	has the meaning given in Paragraph 6.2(a) of Schedule 25 (<i>Exit Management</i>);
“Transferring Authority Employees”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);

“Transferring Former Supplier Employees”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Transferring Supplier Employees”	has the meaning given in Schedule 28 (<i>Staff Transfer</i>);
“Transparency Information”	has the meaning given in Clause 20.1 (Transparency and Freedom of Information);
“Transparency Reports”	has the meaning given in Schedule 24 (<i>Reports and Records Provisions</i>);
“UK”	the United Kingdom;
“UK GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019
“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations;
“Unconnected Sub-contract”	any contract or agreement which is not a Sub-contract and is between the Supplier and a third party (which is not an Affiliate of the Supplier) and is a qualifying contract under regulation 6 of The Reporting on Payment Practices and Performance Regulations 2017;
“Unconnected Sub-contractor”	any third party with whom the Supplier enters into an Unconnected Sub-contract;
“Unrecovered Payment”	has the meaning given in Schedule 16 (<i>Payments on Termination</i>);
“Updates”	in relation to any Software and/or any Deliverable means a version of such item which has been

produced primarily to overcome Defects in, or to improve the operation of, that item;

“Update Requirement” means the occurrence of an event detailed in Schedule 24 (*Reports and Records Provisions*) (Annex 3: *Records To Upload To Virtual Library*) which requires the Supplier to update the relevant information hosted on the Virtual Library;

“Upgrades” any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the Term;

“Valid” in respect of an Assurance, has the meaning given to it in Paragraph 2.7 of Part B to Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*);

“VAT” value added tax as provided for in the Value Added Tax Act 1994;

“VCSE” means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;

“Virtual Library” means the data repository hosted by the Supplier containing the information about this Contract and the Services provided under it in accordance with Schedule 24 (*Reports and Records Provisions*); and

“Working Day” any day other than a Saturday, Sunday or public holiday in England and Wales.

SCHEDULE 2

SERVICES DESCRIPTION

Schedule 2 (Services Description)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

<i>Business Day</i>	Working days are defined as any day other than a Saturday, Sunday or public holiday in England.
<i>Computing Quality Framework</i>	An online tool for school leaders to benchmark their computing provision, identify next steps and demonstrate progress in line with Ofsted. It directs schools to the appropriate parts of the NCCE offer and helps computing hubs to match their support to a school's needs as well as offering an accredited Computing Quality Mark.
<i>Core Hours</i>	Core hours for the NCCE website are set at Monday to Friday 09:00–21:00.

2 INTRODUCTION

For the detailed reasoning behind the procurement of the Contract, please see Document 2 of the invitation to tender pack. A summary of the reasons for the procurement are provided below.

The NCCE 2 aims to improve the quality and impact of computing teaching in primary and secondary state-maintained schools and colleges in England, so that all pupils, regardless of their background, leave school with the digital knowledge and skills they need to participate in a digital society and access the jobs of the future. NCCE 2 will build on the work of the current National Centre ('NCCE 1').

Demand for digital skills: The demand for digital skills continues with computing and digital skills in high demand in the workplace, and this demand is projected to increase. Moreover, employers consistently report persistent skills gaps and there is a perception that there will be digital skills shortages in the short to medium term. Government strategy has focused on the importance of a digitally skilled workforce in recent years; there is an ambition for the UK to become a world leader in cyber and to become a science and technology superpower by 2030. Digital skills are not only needed for employment, but for everyday life, at all stages. Services for health, education, finance, shopping, and those delivered by local authorities have all increasingly become dependent on digital delivery.

Entries in qualifications: Data suggests entries to the Computer Science GCSE may now be levelling off after a few years of marked increase following its introduction and ICT's removal. The Computer Science A Level also experienced large increases

during recent years. Current estimates are that, for every 100 additional GCSE entries, there would be an additional eight entries at A level in two years' time.

Barriers to take up and engagement: The proportion of girls taking the Computer Science GCSE and A level remains low even compared to other science, technology, engineering and maths (STEM) entries.

Quality teaching is the single most important in-school factor for improving pupil outcomes and the shift from ICT to computing means this is in question. It created a requirement for teachers to acquire an entirely new body of subject knowledge, such as algorithms, programming and computer networks, within a short space of time and many teachers still lack proficiency and confidence, including at the lower key stages, where primary teachers are non-specialists by default. Many secondary computing teachers (around 64%) do not have a relevant post-A Level qualification, and only 50% of computer science hours are taught by a specialist teacher. As a relatively new subject, teachers often lack an understanding of the most effective teaching approaches. The NCCE has made great progress in identifying what works well, having published its '12 pedagogy principles for computing', but such developments are recent and best practice is not yet widespread.

Attainment: Data shows that higher-attaining students are achieving lower grades for GCSE Computer Science than they do for other STEM subjects, by at least one grade. This poor attainment at GCSE has created a further barrier to take up, with girls twice as likely as boys to report not taking the subject at GCSE because they did not expect to do well. Stakeholders and teachers have reported that many teachers are 'screening' pupils based on attainment, only encouraging those pupils with evidence of good performance in maths to take the subject.

Delivery method: The Authority conducted a SWOT analysis to consider the best way to deliver the new programme, including options in which the Authority would deliver parts of the programme or for the programme to offer limited number of regional hubs or resources. The Authority's preferred option is for an external supplier to deliver the programme.

- 2.1 This Schedule sets out the intended scope of the Services to be provided by the Supplier and to provide a description of what each Service entails.

3 SERVICES DESCRIPTION

3.1 Implementation Services

Full details of the requirements for the implementation services are set out in Schedule 13 (Implementation Plan). A summary is provided below:

The Supplier shall set up and mobilise the NCCE 2 as a virtual national centre from the Implementation Services Commencement Date to the Operational Services Commencement Date. The Supplier will put in place governance processes and resources in accordance with a critical path and Implementation Plan (they should include all Implementation Milestones linked to Implementation Milestone Payment Dates). The Authority will review the critical path before the Contract starts. The Supplier will work in collaboration with the current supplier(s) to transition the assets and services for the Operational

Services Commencement Date. The Supplier must develop a reporting dashboard for the Implementation Plan; the dashboard will be presented monthly to the Authority to keep the Authority informed and to measure progress. The Supplier must also have a resource plan, a Risk Register and put in place Grant Funding Agreements with each Computing Hub. The Risk Register must be part of the reporting dashboard.

3.2 Operational Services

The Services below are linked to the functions described in detail in the invitation to tender documentation.

Function B: The Supplier shall maintain, manage and monitor the national network of up to 34 high-quality Computing Hubs, including maintaining geographical coverage, and supporting and challenging Computing Hub activity to meet programme KPIs. The Supplier shall improve engagement with the programme and computing in general using Computing Hubs and regional teams at both pupil and teacher level, especially among girls. The Supplier must evaluate the Computing Hubs' activity and ensure coherence, consistency, and clarity across hubs and seek continuous improvement.

The Supplier must implement an engagement plan and bespoke Computing Hub marketing and engagement plans to increase engagement through the hub network and to meet policy objectives of the NCCE 2. They should also work towards to a school engagement plan to provide the specialist computing subject matter expertise and individual support schools need, which may have been identified as part of bespoke action plans or the Computing Quality Framework. The Supplier will fund flow management to the Computing Hubs through grant management and administration.

Function C: The Supplier will promote and increase attainment of continuous professional development to certification standards. The Supplier must deliver the facilitated primary and secondary computing CPD courses set out in the NCCE Asset Register, to computing teachers of all experience and knowledge levels. They must also deliver the student-facing events and teacher-facing facilitated CPD sessions which accompany the GCSE and A Level platform. CPD delivery must be flexible and convenient for teachers.

The Supplier shall provide a continuous improvement function, ensuring that computing education standards improve over the Term of the Contract. The Supplier shall apply the quality assurance function to audit the provision of high-quality computing education.

The Supplier must maintain the existing facilitated NCCE CPD courses, CPD certification programmes and their associated pathways, teacher CPD sessions associated with the GCSE and A Level platforms, and student events associated with the GCSE and A Level platforms, over time so that they remain relevant to the current computing and digital landscape. This includes, for example, ensuring that references to any software, social media platforms and information technology within any course materials do not become outdated.

Schedule 2 (Services Description)

The Supplier must design, create and implement a new gender insights CPD programme for teachers of key stage 3 pupils in mixed and girls' schools. This must support teachers in breaking down barriers to girls' engagement with computing, and to encourage take up of GCSE Computer Science. The programme must comprise high quality resources and CPD based on pedagogical approaches to support girls' engagement with the subject.

The Supplier must present an 'all-through' user journey for teachers who participate in facilitated CPD courses or sessions which accompany the GCSE and A Level platform. This shall start from the booking experience to the consolidation of learning in their school.

The Supplier must support teachers in embedding and consolidating their CPD learning into their teaching practice once completed, through a Computing Hub or other method. The Supplier must make use of the existing NCCE1 'gap tasks', where available as part of CPD courses, in meeting this requirement.

The Supplier may propose new resources or content to complement the NCCE offer in accordance with clause 13 (Change) and Schedule 22 (Change Control Procedure). The proposal of such new content is optional and will be kept to a minimum.

Function D: The Supplier will develop a website promoting the NCCE, utilising existing resources provided under licence, to underpin the programme in schools and colleges. The Supplier must provide the percentage availability and usage of all resources as well as information in aggregate form about the characteristics of users in the Performance Monitoring Report. See Schedule 3 (Performance Levels) of this for the full performance monitoring requirements.

The Supplier will develop and maintain the digital components and ensure all assets are maintained in accordance with the licence agreement and new products are subject to Crown IPR in accordance with Schedule 32 (Intellectual Property Rights). The Supplier must manage the required third party licences as part of ongoing service provision starting from Operational Services Commencement Date.

The Supplier must implement a Service Continuity Plan that incorporates a Disaster Recovery Plan.

The Supplier must ensure they are compliant with Data Protection Legislation. When developing, maintaining and implementing the IT services, the Supplier must adhere to: accessibility standards; assessment and assurance standards; security standards; portability standards; reliability, resilience and disaster recovery standards; child safeguarding standards; performance standards; interoperability standards, and availability standards.

Function E: The Supplier shall provide policy and stakeholder expertise on computing education and engage with industry and the education sector.

The Supplier will ensure the programme does not become outdated and the work of the NCCE 2 is based on the latest and most effective evidence-based computing pedagogy.

Schedule 2 (Services Description)

The Supplier will provide objective, unbiased professional support and knowledge for a range of departmental requirements. The Supplier will engage proactively with industry and other government departments (OGDs) to promote the NCCE 2 and advance computing education in England. Through industry engagement, the Supplier will use their expertise to understand the impact of the NCCE 2 on the wider digital skills agenda and will inform the Authority of any emerging gaps.

The Supplier will plan and deliver outreach activities and industry events within schools and educational establishments, either organised through Isaac or with professional advisors/charities. The Supplier will engage with nationally recognised competitions and events to promote computer science in schools and colleges. They should also raise awareness of the NCCE 2, as well as the achievements of the NCCE 1, to encourage more young people into computing careers.

Function F: The Supplier must provide project management for all corporate functions of the programme including resourcing, governance, compliance, assurance, financial management, reporting and monitoring/delivering against KPIs. This should extend to supply chains, that are Key Sub-contractors.

The Supplier must implement a delivery plan with a critical path (aligned to KPIs) to enable Service delivery to commence from Operational Services Commencement Date in line with all functions specified in the ITT.

The Supplier must have an Exit Plan Asset Register and all necessary documentation. The Supplier must ensure the NCCE 2 is appropriately resourced and maintain the asset register, the TUPE register and a Risk Register. They will also develop and implement a marketing and communications strategy that also covers Contract end and exit.

The Supplier will develop a comprehensive reporting dashboard that incorporates all Performance Monitoring Report information and reporting data across the programme. They will present the dashboard monthly to ensure the Authority is informed of progress against delivery/KPIs/financial spend.

The Supplier will work with an independent evaluator to provide information and assistance in a timely manner to evaluate the impact of the programme.

Function G: see social value (3.5 below)

Ad hoc requests: The Supplier is required to provide information specified by the Authority, or Subcontractor appointed by the Authority to conduct an evaluation of the Services, in accordance with such timescales and at such intervals as may be specified in the Supplier's delivery plans or as may be reasonably required from time to time by the Authority, the National Audit Office or any evaluation contractor appointed by the Authority. The Supplier is required to provide all reasonable support and assistance when officials have urgent Data Requests, such as but not limited to Freedom of Information Act 2000 or Data Protection Legislation, requests from ministers or questions from Members of Parliament. This should be provided at no additional cost to the Authority.

The Supplier must ensure IT services meet uptimes of above 99.5% for both the front-end and back-end systems. The Supplier must report availability and any breach of the service availability requirements set out in Scheduled 3 (Performance Levels) will trigger Service Points to be allocated that Service Period as detailed in Schedule 3 (Performance Levels) and Schedule 15 (Charges and Invoicing) (See ITT pack, Document 3, Statement of Requirements).

The Supplier must ensure that where downtime is required it takes place outside of Core Hours. A notice period of five (5) Working Days is required for downtime affecting user experience and system availability.

3.3 Interface Requirements

- (a) technical interface and
- (b) management obligations/responsibilities

3.4 Security Requirements

See Schedule 5 of this Contract.

3.5 Social Value Requirements

The programme's social value theme is 'Tackling economic inequality' with the policy outcome of creating new businesses, jobs and skills. The Supplier must create and deliver against KPIs related to their social value proposal. The Supplier must create employment opportunities particularly for those who face barriers to employment, those living in deprived areas, and people in industries with known skills shortages and those in jobs in high growth sectors.

3.6 Other Authority Requirements

The Supplier is obliged to adhere to the requirements listed in Schedule 4 (Standards) of this Contract.

SCHEDULE 3

PERFORMANCE LEVELS

Schedule 3 (*Performance Levels*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“End User”	any person authorised by the Authority to use the IT Environment and/or the Services;
“Help Desk”	the single point of contact help desk set up and operated by the Supplier for the purposes of this Contract;
“Performance Monitoring Report”	has the meaning given in Paragraph 1.1(a) of Part B;
“Performance Review Meeting”	the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Contract, as further described in Paragraph 1.5 of Part B;
“Satisfaction Survey”	has the meaning given in Paragraph 1.1 of Part B of Annex 1;
“Service Period”	one calendar month from the Operational Services Commencement Date;

Part A: Performance Indicators and Service Credits

1 PERFORMANCE INDICATORS

- 1.1 Annex 1 sets out the Key Performance Indicators and Subsidiary Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services and Social Value by the Supplier.
- 1.2 The Supplier shall monitor its performance against each Performance Indicator and shall send the Authority a report detailing the level of service actually achieved in accordance with Part B.
- 1.3 The Authority will make the relevant KPI Milestone Payments to the Supplier where the Supplier achieves the KPI Milestone Payment threshold as detailed in Annex 1 of this Schedule. The maximum KPI Milestone Payments to be paid upon the achievement of the KPI Milestone Payment thresholds for each KPI Milestone are set out in Annex 1 of Schedule 15 (Charges and Invoicing).
- 1.4 Service Points shall accrue as detailed in Paragraph 4.1 of this Part A and Part C of Schedule 15 (Charges and Invoicing).

2 KPI FAILURES

- 2.1 If a KPI Failure occurs in respect of the same Key Performance Indicator in any two consecutive Measurement Periods, the second and any subsequent such KPI Failure shall be a “**Repeat KPI Failure**”.
- 2.2 Where a Repeat KPI Failure occurs, the Rectification Plan Process will be followed.

3 PERMITTED MAINTENANCE

- 3.1 The Authority and Supplier agree that Service Downtime for Permitted Maintenance will take place no more than once a month at a time to be agreed, and which shall take place between the hours and on the day specified in the Maintenance Schedule unless otherwise agreed in writing with the Authority.

4 SERVICE AVAILABILITY AND SERVICE CREDITS

- 4.1 The Supplier shall ensure:
 - 4.1.1 IT services meet uptimes of above 99.5% for both the front-end and back end systems; and
 - 4.1.2 where down-time is required, this must take place outside of core hours (Monday to Friday 09.00–21.00)
- 4.2 Where the requirements detailed in paragraphs 4.1.1 and 4.1.2 are breached, Service Points shall be accrued as set out in Part C of Schedule 15 (Charges and Invoicing).
- 4.3 Schedule 15 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.

Schedule 3 (Performance Levels)

- 4.4 The Authority shall use the Performance Monitoring Reports provided pursuant to Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

Part B: Performance Monitoring

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 Within 10 Working Days of the end of each Service Period, the Supplier shall provide:

- (a) a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.2 (the “**Performance Monitoring Report**”); and
- (b) a report created by the Supplier to the Authority’s senior responsible officer which summarises the Supplier’s performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the “**Balanced Scorecard Report**”).

Performance Monitoring Report

1.2 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

- (a) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the Service Period, and that achieved over the previous 3 Measurement Periods;
- (b) a summary of all Performance Failures that occurred during the Service Period;
- (c) the severity level of each KPI Failure which occurred during the Service Period and whether each PI Failure which occurred during the Service Period fell below the PI Service Threshold;
- (d) which Performance Failures remain outstanding and progress in resolving them;
- (e) for any Repeat KPI Failure occurring during the Service Period, the cause of the relevant KPI Failure and the action being taken to reduce the likelihood of recurrence;
- (f) the status of any outstanding Rectification Plan processes, including:
 - (i) whether or not a Rectification Plan has been agreed; and
 - (ii) where a Rectification Plan has been agreed, a summary of the Supplier’s progress in implementing that Rectification Plan;
- (g) for any recurring Performance Failures, actions taken to resolve the underlying cause and prevent recurrence;
- (h) the number of Service Points accrued;

Schedule 3 (Performance Levels)

- (i) the Service Credits to be applied;
- (j) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;
- (k) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Contract;
- (l) in respect of the website created the percentage availability and usage of all resources as well as information in the aggregate form about the characterises of users;
- (m) such other details as the Authority may reasonably require from time to time; and

Information in respect of previous Service Periods

- (a) a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;
- (b) the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;
- (c) the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan; and

Information in respect of the next Quarter

- (a) any scheduled Service Downtime for Permitted Maintenance and Updates that has been agreed between the Authority and the Supplier for the next Quarter.

Balanced Scorecard Report

1.2 The Balanced Scorecard Report shall be presented in the form of an online accessible dashboard and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period, including details of the following:

- (a) financial indicators;
- (b) the Target Performance Levels achieved;
- (c) behavioural indicators;
- (d) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;
- (e) performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice;
- (f) Milestone trend chart, showing performance of the overall programme;

Schedule 3 (Performance Levels)

- (g) sustainability indicators, for example net zero carbon, waste minimisation or performance to support a circular economy; and
 - (h) Social Value (as applicable).
- 1.3 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Meeting held in accordance with Paragraph 1.5.
- 1.4 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Scorecard Reports. The Performance Review Meetings shall (unless otherwise agreed):
 - (a) take place within 5 Working Days of the Performance Monitoring Report being issued by the Supplier;
 - (b) take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and
 - (c) be attended by the Supplier Representative and the Authority Representative.
- 1.5 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure and/or PI Failure.

2 PERFORMANCE RECORDS

- 2.1 The Supplier shall keep appropriate documents and records (including Help Desk records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.
- 2.2 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.
- 2.3 The Supplier shall ensure that the Performance Monitoring Report, the Balanced Scorecard Report (as well as historic Performance Monitoring Reports and historic Balance Scorecard Reports) and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.

3 PERFORMANCE VERIFICATION

- 3.1 The Authority reserves the right to verify the Availability of the IT Environment and/or the Services and the Supplier's performance under this Contract against the Performance Indicators including by sending test transactions through the IT Environment or otherwise.

Annex 1: Key Performance Indicators and Subsidiary Performance Indicators

Part A: Key Performance Indicators and Subsidiary Performance Indicators Tables

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Operational Services and the Key Performance Indicators relating to Social Value are set out below:

1 Key Performance Indicators

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
1						
2						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
3						
4						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
5						
6						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
7						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
8						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
9						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information
10						
11						

Schedule 3 (Performance Levels)

KPI No.	Key Performance Indicator title	Definition	Monitoring method and frequency of measurement	Target Performance Level	KPI Milestone Payment threshold	Publishable Performance Information

2 **Subsidiary Performance Indicators**

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Threshold	Publishable Performance Information
PI1					
PI2					

Annex 1

Part B:

1 SATISFACTION SURVEYS

- 1.1 In order to assess the level of performance of the Supplier, the Authority may undertake satisfaction surveys in respect of End Users or various groups of End Users (each such survey a “**Satisfaction Survey**”), the results of which may be reflected in the Balanced Scorecard Report. The subject matter of Satisfaction Surveys may include:
- (a) the assessment of the Supplier’s performance by the End Users against the agreed Key Performance Indicators and Subsidiary Performance Indicators; and/or
 - (b) other suggestions for improvements to the Services.
- 1.2 The Authority shall reflect in the Balanced Scorecard Report any aspects of the Supplier’s performance of the Services which the responses to the Satisfaction Surveys reasonably suggest are not meeting the Services Description.

2 VIRTUAL LIBRARY COMPLETENESS

- 2.1 The Virtual Library shall be complete where all of the information required under Schedule 24 (Reports and Records Provisions) (Annex 3: Records To Upload To Virtual Library)) has been uploaded to the Virtual Library in accordance with Paragraph 3 of that Schedule.

SCHEDULE 4

STANDARDS

Schedule 4 (*Standards*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Standards Hub”	the Government’s open and transparent standards adoption process as documented at http://standards.data.gov.uk/ ; and
“Suggested Challenge”	a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2 GENERAL

- 2.1 Throughout the Term of this Contract, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier’s provision, or the Authority’s receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.
- 2.2 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier’s provision, or the Authority’s receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
- 2.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

3 TECHNOLOGY AND DIGITAL SERVICES PRACTICE

- 3.1 The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government’s Technology Code of Practice as documented at <https://www.gov.uk/service-manual/technology/code-of-practice.html>.

4 OPEN DATA STANDARDS & STANDARDS HUB

- 4.1 The Supplier shall comply to the extent within its control with UK Government’s Open Standards Principles as documented at <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.
- 4.2 Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or

Supplier Solution where there is a requirement under this Contract or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at <http://standards.data.gov.uk/>). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Contract, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

- 4.3 The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Contract is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

5 TECHNOLOGY ARCHITECTURE STANDARDS

- 5.1 The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable.

6 ACCESSIBLE DIGITAL STANDARDS

- 6.1 The Supplier shall comply with (or with equivalents to):
- (a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and
 - (b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

7 SERVICE MANAGEMENT SOFTWARE & STANDARDS

- 7.1 Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:
- (a) ITIL v4;
 - (b) ISO/IEC 20000-1 2018 "Information technology — Service management – Part 1";
 - (c) ISO/IEC 20000-2 2019 "Information technology — Service management – Part 2";
 - (d) ISO/IEC 27001/27002 "Information security management"

Schedule 4 (Standards)

- (e) ISO 10007: 2017 “Quality management systems – Guidelines for configuration management”;
- (f) ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019
- (g) Government Digital Standards - [Government Digital Service - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/digital-standards) - [Service Standard - Service Manual - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/service-standard); and
- (h) Technology code of practice - [The Technology Code of Practice - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/technology-code-of-practice).

7.2 For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.

8 SUSTAINABILITY

8.1 The Supplier shall comply with the sustainability requirements set out in the Annex to this Schedule.

9 HARDWARE SAFETY STANDARDS

9.1 The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:

- (a) any new hardware required for the delivery of the Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;
- (b) any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN IEC 62368-1:2020+A11:2020 or any subsequent replacements;
- (c) any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2014 or any subsequent replacements; and
- (d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 62949:2017 or any subsequent replacements.

Schedule 4 (Standards)

- 9.2 Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Contract in accordance with the relevant health and safety regulations.

ANNEX 1: SUSTAINABILITY

1 DEFINITIONS

1.1 In this Annex, the following definitions shall apply:

“Permitted Item”	means those items which are permissible under this Contract to the extent set out in Table B of this Annex
“Prohibited Items”	means those items which are not permissible under this Contract as set out at Table A of this Annex
“Sustainability Reports”	written reports to be completed by the Supplier containing the information outlined in Table C of this Annex
“Waste Hierarchy”	<p>means prioritisation of waste management in the following order of preference as set out in the Waste (England and Wales) Regulation 2011:</p> <ul style="list-style-type: none">(a) Prevention;(b) Preparing for re-use;(c) Recycling;(d) Other Recovery; and(e) Disposal.

2 PUBLIC SECTOR EQUALITY DUTY

2.1 In addition to legal obligations, where the Supplier is providing a Service to which the Public Sector Equality duty applies, the Supplier shall support the Authority in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under the Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation and any other conduct prohibited by the Equality Act 2010; and

2.1.2 advance:

- (a) equality of opportunity; and
- (b) good relations,

between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

Schedule 4 (Standards)

- 2.2 In delivering the Service, the Supplier will comply with the Authority's equality, diversity and inclusion requirements, to be provided to the Supplier by the Authority.
- 2.3 The Supplier shall ensure that it fulfils its obligations under the Contract in a way that does not discriminate against individuals because of socio-economic background, working pattern or having parental or other caring responsibilities.

3 ENVIRONMENTAL REQUIREMENTS

- 3.1 The Supplier must perform its obligations meeting in all material respects the requirements of all applicable Laws regarding the environment.
- 3.2 The Supplier warrants that it has obtained relevant Environment Management System (EMS) certified to ISO 14001 or an equivalent certification from a UKAS accredited body and shall comply with and maintain certification requirements throughout the Term.
- 3.3 In performing its obligations under the Contract, the Supplier shall, where applicable to the Contract, to the reasonable satisfaction of the Authority:
 - (a) demonstrate low carbon resource efficiency, including minimising the use of resources and responding promptly to the Authority's reasonable questions;
 - (b) prioritise waste management in accordance with the Waste Hierarchy as set out in Law;
 - (c) be responsible for ensuring that any waste generated by the Supplier and sent for recycling, disposal or other recovery as a consequence of this Contract is taken by a licensed waste carrier to an authorised site for treatment or disposal and that the disposal or treatment of waste complies with the law;
 - (d) ensure that it and any third parties used to undertake recycling disposal or other recovery as a consequence of this Contract do so in a legally compliant way, and can demonstrate that reasonable checks are undertaken to ensure this on a regular basis and provide relevant data and evidence of recycling, recovery and disposal;
 - (e) in circumstances that a permit, licence or exemption to carry or send waste generated under this Contract is revoked, the Supplier shall cease to carry or send waste or allow waste to be carried by any Subcontractor until authorisation is obtained from the Environment Agency; minimise the release of greenhouse gases (including carbon dioxide emissions), air pollutants, volatile organic compounds and other substances damaging to health and the environment; and
 - (f) reduce and minimise carbon emissions by taking into account factors including, but not limited to, the locations from which materials are sourced, the transport of materials, the locations from which the work force are recruited and emissions from offices and on-site equipment.

Schedule 4 (Standards)

- 3.4 In performing its obligations under the Contract, the Supplier shall to the reasonable satisfaction of the Authority (where the anticipated Charges in any Contract Year are above £5 million per annum (excluding VAT)), where related to and proportionate to the contract in accordance with PPN 06/21), publish and maintain a credible Carbon Reduction Plan in accordance with PPN 06/21.
- 3.5 The Supplier shall not provide to the Authority Goods or Deliverables which comprise wholly or partly of Prohibited Items unless such item is a Permitted Item.
- 3.6 The Supplier shall not use anything which comprises wholly or partly of the Prohibited Items to provide the Services under this Contract unless:
- (a) it is a Permitted Item; or
 - (b) the use is primarily related to the management of the Supplier's own facilities or internal operations as opposed to the provision of Services.
- 3.7 The Supplier must have a documented management system and controls in place to manage the environmental impacts of delivering the Services.
- 3.8 The Supplier shall ensure that any Services are designed, sourced and delivered in a manner which is environmentally and socially responsible.
- 3.9 In delivering the Services, the Supplier must comply with the Authority's sustainability requirements, to be provided to the Supplier by the Authority.
- 3.10 In performing its obligations under the Contract, the Supplier shall to the reasonable satisfaction of the Authority:
- 3.10.1 demonstrate that the whole life cycle impacts (including end of use) associated with the Services that extend beyond direct operations into that of the supply chain have been considered and reduced];
 - 3.10.2 minimise the consumption of resources and use them efficiently (including water and energy), working towards a circular economy including designing out waste and non-renewable resources, using re-use and closed loop systems;
 - 3.10.3 demonstrate protection of the environment including understanding and reduction of biosecurity risks (which include risks to plant and tree health from harmful pests and diseases), and reducing and eliminating hazardous/harmful substances to the environment and preventing pollution];
 - 3.10.4 enhance the natural environment and connecting communities with the environment]; and
 - 3.10.5 achieve continuous improvement in environmental (and social) performance.]]
 - 3.10.6 - 3.10.10 is not applicable and has been deleted.

Schedule 4 (Standards)

3.11 The Supplier shall inform the Authority within one Working Day in the event that a permit, licence or exemption to carry or send waste generated under this Contract is revoked.

3.12 Not used

3.13 The Supplier shall meet the applicable Government Buying Standards applicable to Services which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>.

4 SUPPLIER CODE OF CONDUCT

4.1 In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government which can be found online at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier Code of Conduct.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf)

The Authority expects to meet, and expects its suppliers and subcontractors to meet, the standards set out in that Code.

5 REPORTING REQUIREMENTS

5.1 The Supplier shall comply with reasonable requests by the Authority for information evidencing compliance:

5.1.1 with Paragraphs 2.1, 3.1 to 3.6, 3.13 and 4 of this Annex within fourteen (14) days of such request; and

5.1.2 With Paragraphs 2.2, 2.3 and 3.7 to 3.12 of this Annex within thirty (30) days of such request,

provided that such requests are limited to two per Contract Year.]

5.2 The Supplier shall complete the Sustainability Report in relation its provision of the Services under this Contract and provide the Sustainability Report to the Authority on the date and frequency outlined in Table C of this Annex.

TABLE A – PROHIBITED ITEMS

<p>The following consumer single use plastics are Prohibited Items:</p>	
	<p>Facilities</p> <ul style="list-style-type: none"> a. Single use containers e.g. hand soap, cleaning products b. Wipes containing plastic
	<p>Office Supplies</p> <ul style="list-style-type: none"> a. Plastic envelopes b. Plastic wrapping for brochures c. Paper or card which is bleached with chlorine
	<p>Packaging</p> <ul style="list-style-type: none"> a. Single use plastic packaging from deliveries where avoidable e.g. shrink wrapped packaging from office supplier or facilities products. b. Single use carrier bags

Schedule 4 (Standards)

TABLE B – PERMITTED ITEMS

NOT USED

TABLE C – SUSTAINABILITY REPORTS

Sustainability Report Name	Content of Report	Frequency of Report
Sustainability - General	[as proportionate and relevant to the Contract, the key sustainability impacts identified; the sustainability improvements planned or delivered; and the risks to the Services of climate change, including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks].	On the anniversary of the Effective Date
<u>ICT and Digital footprint</u>	<u>The Supplier should deliver annual ICT and digital footprint waste and best practice data report for each department / partner organisation</u>	<u>Annual report from Operational Services Commencement Date</u>

SCHEDULE 5

SECURITY MANAGEMENT

Schedule 5 (Security Management)

PART A: SECURITY ASSURANCE

1 Definitions

1.1 In this Schedule:

“Anti-Malicious Software”	means software that scans for and identifies possible Malicious Software in the IT Environment;
“Breach of Security”	(a) an event that results, or could result, in: (a) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or (b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Contract;
“Certification Requirements”	means the information security requirements set out in Paragraph 6;
“CHECK Service Provider”	means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 7.1;
“CREST Service Provider”	means a company with a SOC Accreditation from CREST International;
“Higher Risk Sub-contractor”	means a Sub-contractor and Computing Hub that Processes Authority Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); or (b) any part of that data includes any of the following:

- (i) financial information (including any tax and/or welfare information) relating to any person;
- (ii) any information relating to actual or alleged criminal offences (including criminal records);
- (iii) any information relating to children and/or vulnerable persons;
- (iv) any information relating to social care;
- (v) any information relating to a person's current or past employment; or
- (vi) Special Category Personal Data; or
- (c) the Authority in its discretion, designates a Sub-contractor or Computing Hub as a Higher Risk Sub-Contractor in any procurement document related to this Contract; or
- (d) the Authority considers in its discretion, that any actual or potential Processing carried out by the Sub-contractor or Computing Hub is high risk

“Cyber Essentials” means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;

“Cyber Essentials Plus” means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;

“Cyber Essentials Scheme” means the Cyber Essentials scheme operated by the National Cyber Security Centre;

“Incident Management Process” means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 4 using the template set out in Annex 3;

“Information Assurance Assessment” means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 4 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches

and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3;

“Information Management System”

means

- (a) those parts of the Supplier System, and those of the Sites, that the Supplier or its Sub-contractors or Computing Hubs will use to provide the parts of the Services that require Processing Authority Data; and
- (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);

“Information Security Approval Statement”

means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that:

- (a) the Authority is satisfied that the identified risks have been adequately and appropriately addressed;
- (b) the Authority has accepted the residual risks; and
- (c) the Supplier may use the Information Management System to Process Authority Data;

“IT Health Check”

has the meaning given in Paragraph 7.1(a);

“Medium Risk Sub-contractor”

means a Sub-contractor and Computing Hub that Processes Authority Data, where that data

- (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the first Operational Service Commencement Date and the date on which this Contract terminates in accordance with Clause 4.1(b); and
- (b) does not include Special Category Personal Data;

“Process”

means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

	dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“Remediation Action Plan”	has the meaning given in Paragraph 7.3(c)(i);
“Required Changes Register”	mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 5.2 together with the date by which such change shall be implemented and the date on which such change was implemented;
“Risk Register”	is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Authority for approval in accordance with Paragraph 4;
“Security Management Plan”	means the document prepared by the Supplier using the template in Annex 3, comprising: <ul style="list-style-type: none">(a) the Information Assurance Assessment;(b) the Required Changes Register; and(c) the Incident Management Process;
Special Category Personal Data	means the categories of Personal Data set out in article 9(1) of the UK GDPR;

2 Introduction

2.1 This **Part A** of this Schedule sets out:

- (a) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Authority Data and the Information Management System;
- (b) the Certification Requirements applicable to the Supplier and each of those Sub-contractors and Computing Hubs which Process Authority Data;
- (c) the security requirements in Annex **1**, with which the Supplier must comply;

Schedule 5 (Security Management)

- (d) the tests which the Supplier shall conduct on the Information Management System during the Term; and
- (e) the Supplier's obligations to:
 - (i) return or destroy Authority Data on the expiry or earlier termination of this Contract; and
 - (ii) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 9; and
 - (iii) report Breaches of Security to the Authority.

3 Principles of Security

- 3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:
 - (a) the Sites;
 - (b) the IT Environment;
 - (c) the Information Management System; and
 - (d) the Services.
- 3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:
 - (a) the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors or any of the Computing Hubs; and
 - (b) the security of the Information Management System.
- 3.3 The Supplier shall:
 - (a) comply with the security requirements in Annex 1; and
 - (b) ensure that each Sub-contractor and Computing Hub that Processes Authority Data complies with Annex 1.
- 3.4 The Supplier shall provide the Authority with access to Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

4 Information Security Approval Statement

- 4.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule, including any requirements imposed on Sub-contractors and Computing Hubs by Annex 2, from the first Operational Services Commencement Date.
- 4.2 The Supplier may not use the Information Management System to Process Authority Data unless and until:
- (a) the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 7.1; and
 - (b) the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 4.
- 4.3 The Supplier shall document in the Security Management Plan how the Supplier, its Sub-contractors and the Computing Hubs shall comply with the requirements set out in this Schedule and the Contract in order to ensure the security of the Authority Data and the Information Management System.
- 4.4 The Supplier shall prepare and submit to the Authority within 20 Working Days of the date of this Contract, the Security Management Plan, which comprises:
- (a) an Information Assurance Assessment;
 - (b) the Required Changes Register; and
 - (c) the Incident Management Process.
- 4.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:
- (a) an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or
 - (b) a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.
- 4.6 If the Authority rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Authority for review within 10 Working Days or such other timescale as agreed with the Authority.
- 4.7 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:
- (a) access to the Supplier Personnel;

- (b) access to the Information Management System to audit the Supplier and its Sub-contractors' and Computing Hubs compliance with this Contract; and
- (c) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Supplier, its Sub-contractors and Computing Hubs have implemented in order to ensure the security of the Authority Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Authority in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Authority with the access that it requires within 24 hours of receipt of such request.

5 Compliance Reviews

- 5.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this Paragraph.
- 5.2 The Supplier shall notify the Authority within [2] Working Days after becoming aware of:
 - (a) a significant change to the components or architecture of the Information Management System;
 - (b) a new risk to the components or architecture of the Information Management System;
 - (c) a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph 9.2 of Annex 1 to this Schedule;
 - (d) a change in the threat profile;
 - (e) a significant change to any risk component;
 - (f) a significant change in the quantity of Personal Data held within the Service;
 - (g) a proposal to change any of the Sites from which any part of the Services are provided; and/or
 - (h) an ISO/IEC 27001 (at least ISO/IEC 27001:2013) audit report produced in connection with the Certification Requirements indicates significant concerns.
- 5.3 Within 10 Working Days of such notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary

changes to the Required Changes Register and submit the updated Required Changes Register the Authority for review and approval.

- 5.4 Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost and expense.

6 Certification Requirements

- 6.1 The Supplier shall be certified as compliant with:

(a) ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and

(b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.

- 6.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:

(a) ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);

(b) Cyber Essentials PLUS; or

(c) [Cyber Essential \(if it has less than 250 employees\)](#),

and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.

- 6.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.

- 6.4 The Supplier shall ensure that the Supplier and each Sub-contractor and Computing Hub who is responsible for the secure destruction of Authority Data:

(a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);

(b) should satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

(c) must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

Schedule 5 (Security Management)

- 6.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's and Computing Hubs compliance with the requirements set out in this Paragraph 6 before the Supplier or the relevant Sub-contractor or Computing Hub (as applicable) may carry out the secure destruction of any Authority Data.
- 6.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier, any Sub-contractor or Computing Hub ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor or Computing Hub shall:
- (a) immediately ceases using the Authority Data; and
 - (b) procure that the relevant Sub-contractor or Computing Hub promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph.
- 6.7 The Authority may agree to exempt, in whole or part, the Supplier, any Sub-contractor or Computing Hub from the requirements of this Paragraph 6. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

7 Security Testing

- 7.1 The Supplier shall, at its own cost and expense procure and conduct:
- (a) testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and
 - (b) such other security tests as may be required by the Authority,
- 7.2 The Supplier shall:
- (a) complete all of the above security tests before:
 - (i) the Supplier submits the Security Management Plan to the Authority for review in accordance with Paragraph 4; and
 - (ii) before the Supplier is given permission by the Authority to Process or manage any Authority Data; and
 - (b) repeat the IT Health Check not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with this Paragraph.
- 7.3 In relation to each IT Health Check, the Supplier shall:
- (a) agree with the Authority the aim and scope of the IT Health Check;
 - (b) promptly, and no later than ten (10) Working Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

- (c) in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
 - (i) prepare a remedial plan for approval by the Authority (each a **"Remediation Action Plan"**) which sets out in respect of each vulnerability identified in the IT Health Check report:
 - (A) how the vulnerability will be remedied;
 - (B) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:
 - (1) within three months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "medium";
 - (2) within one month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "high"; and
 - (3) within 7 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "critical";
 - (C) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (ii) comply with the Remediation Action Plan; and
 - (iii) conduct such further tests on the Service as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has been complied with.
- 7.4 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.
- 7.5 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Authority with a copy of the test report and:
- (a) propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and

- (b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

7.6 The Supplier shall conduct such further tests of the Supplier System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Contract.

7.7 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 7.3.

8 Security Monitoring and Reporting

8.1 The Supplier shall:

- (a) monitor the delivery of assurance activities;
- (b) maintain and update the Security Management Plan in accordance with Paragraph 5;
- (c) agree a document which presents the residual security risks to inform the Authority's decision to give approval to the Supplier to Process and transit the Authority Data;
- (d) monitor security risk impacting upon the operation of the Service;
- (e) report Breaches of Security in accordance with the approved Incident Management Process;
- (f) agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 20 Working Days of Effective Date.

9 Malicious Software

9.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 9.2 shall be borne by the parties as follows:

- (a) by the Supplier where the Malicious Software originates from:
 - (i) the Supplier Software;
 - (ii) the Third Party Software supplied by the Supplier; or
 - (iii) the Authority Data whilst the Authority Data is or was under the control of the Supplier,

unless, in the case of the Authority Data only, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and

- (b) by the Authority, in any other circumstance.

10 Breach of Security

10.1 If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

10.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

- (a) Immediately take all reasonable steps necessary to:
 - (i) minimise the extent of actual or potential harm caused by such Breach of Security;
 - (ii) remedy such Breach of Security to the extent possible;
 - (iii) apply a tested mitigation against any such Breach of Security; and
 - (iv) prevent a further Breach of Security in the future which exploits the same root cause failure;
- (b) as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

10.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and Computing Hubs and/or all or any part of the Information Management System with this Contract, then such remedial action shall be completed at no additional cost to the Authority.

ANNEX 1: SECURITY REQUIREMENTS

1 Security Classification of Information

- 1.1 If the provision of the Services requires the Supplier to Process Authority Data which is classified as:
- (a) **OFFICIAL-SENSITIVE**, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or
 - (b) **SECRET or TOP SECRET**, the Supplier shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 End User Devices

- 2.1 The Supplier must manage, and must ensure that all Sub-contractors and Computing Hubs manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance the following requirements:
- 2.1.1 the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;
 - 2.1.2 users must authenticate before gaining access;
 - 2.1.3 all Authority Data must be encrypted using an encryption tool agreed to by the Authority;
 - 2.1.4 the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
 - 2.1.5 the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;
 - 2.1.6 the Supplier, Sub-contractor or Computing Hub, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;
 - 2.1.7 all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

Schedule 5 (Security Management)

- 2.2 The Supplier must comply, and ensure that all Sub-contractors and Computing Hubs (as applicable) comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Contract.
- 2.3 Where there any conflict between the requirements of this Schedule 5 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

3 Encryption

- 3.1 The Supplier must ensure, and must ensure that all Sub-contractors and Computing Hubs ensure, that Authority Data is encrypted:
 - 3.1.1 when stored at any time when no operation is being performed on it; and
 - 3.1.2 when transmitted.
- 3.2 Where the Supplier, a Sub-contractor, or Computing Hub cannot encrypt Authority Data the Supplier must:
 - 3.2.1 immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 3.2.2 provide details of the protective measures the Supplier, Sub-contractor or Computing Hub (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - 3.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.
- 3.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-contractor or Computing Hub shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 3.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
 - 3.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and
 - 3.4.2 the protective measure that the Supplier, Sub-contractor and/or Computing Hub will put in place in respect of the unencrypted Authority Data.
- 3.5 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.

4 Personnel Security

- 4.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.
- 4.2 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.
- 4.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
- 4.4 The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
- 4.5 The Supplier shall ensure that Supplier Personnel and Computing Hubs who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors or Computing Hubs), have their rights to access the Authority Data revoked within 1 Working Day.
- 4.6 The Supplier shall ensure that Supplier Personnel and Computing Hubs that have access to the Sites, the IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Authority Data.
- 4.7 The Supplier shall ensure that the training provided to Supplier Personnel and Computing Hubs under Paragraph 4.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Authority Data ("phishing").

5 Identity, Authentication and Access Control

- 5.1 The Supplier shall operate an access control regime to ensure:

Schedule 5 (Security Management)

- (a) all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
 - (b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
- 5.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.
- 5.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.

6 Data Destruction or Deletion

- 6.1 The Supplier shall:
 - (a) prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Government with all Authority Data in an agreed open format;
 - (b) have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;
 - (c) securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;
 - (d) securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as agreed by the Authority; and
 - (e) implement processes which address the CPNI and NCSC guidance on secure sanitisation.

7 Audit and Protective Monitoring

- 7.1 The Supplier shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.
- 7.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Information Management System.
- 7.3 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security Management Plan.

8 Location of Authority Data

- 8.1 The Supplier shall not and shall procure that none of its Sub-contractors or any Computing Hubs Process Authority Data outside the EU without the prior written consent of the Authority, which may be subject to conditions.

9 Vulnerabilities and Corrective Action

- 9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

- 9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

- (a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at <http://nvd.nist.gov/cvss.cfm>); and
- (b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

- 9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

- (a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';
- (b) thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important'; and
- (c) sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Other'.

- 9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 9.3 shall be extended where:

- (a) the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;
- (b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of five (5) days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

- (c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

9.5 The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing. All COTS Software should be no more than N-1 versions behind the latest software release.

10 Secure Architecture

10.1 The Supplier shall design the Information Management System in accordance with:

- (a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;
- (b) the NCSC "Bulk Data Principles", a copy of which can be found at <https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main>; and
- (c) the NSCS "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> and which are summarised below:
 - (i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
 - (ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
 - (iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
 - (iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
 - (v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
 - (vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have

access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

- (vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
- (viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers including Computing Hubs ;
- (ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
- (x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
- (xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
- (xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
- (xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors and/or Computing Hubs; and
- (xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS AND COMPUTING HUBS

1 Application of Annex

- 1.1 This Annex applies to all Sub-contractors and Computing Hubs that Process Authority Data.
- 1.2 The Supplier must:
 - (a) ensure that those Sub-contractors and Computing Hubs comply with the provisions of this Annex;
 - (b) keep sufficient records to demonstrate that compliance to the Authority; and
 - (c) ensure that its Implementation Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-contractors and Computing Hubs to Process Authority Data.

2 Designing and managing secure solutions

- 2.1 The Sub-contractor and/or Computing Hub shall implement their solution(s) to mitigate the security risks in accordance with the NCSC's Cyber Security Design Principles <https://www.ncsc.gov.uk/collection/cyber-security-design-principles>.
- 2.2 The Sub-contractor and/or Computing Hub must assess their systems against the NCSC Cloud Security Principles: <https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles> at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Authority on the Authority's request.

3 Data Processing, Storage, Management and Destruction

- 3.1 The Sub-contractor and/or Computing Hub must not Process any Authority Data outside the UK. The Authority may permit the Sub-contractor to Process Authority Data outside the UK and may impose conditions on that permission, with which the Sub-contractor must comply. Any permission must be in writing to be effective.
- 3.2 The Sub-contractor and/or Computing Hub must when requested to do so by the Authority:
 - (a) securely destroy Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);
 - (b) satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

- (c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or **deleted**.

4 Personnel Security

- 4.1 The Sub-contractor and/or Computing Hub must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>.
- 4.2 The Sub-contractor and/or Computing Hub must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.
- 4.3 Any Sub-contractor and/or Computing Hub staff who will, when performing the Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service checks.

5 End User Devices

- 5.1 The Supplier must manage, and must ensure that all Sub-contractors and Computing Hubs manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance the following requirements:
 - 5.1.1 the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;
 - 5.1.2 users must authenticate before gaining access;
 - 5.1.3 all Authority Data must be encrypted using an encryption tool agreed to by the Authority;
 - 5.1.4 the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;
 - 5.1.5 the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;
 - 5.1.6 the Supplier, Sub-contractor or Computing Hub, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;

Schedule 5 (Security Management)

- 5.1.7 all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
- 5.2 The Supplier must comply, and ensure that all Sub-contractors and Computing Hubs comply, with the recommendations in NCSC Device Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Agreement.
- 5.3 Where there any conflict between the requirements of this Schedule 5 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

6 Encryption

- 6.1 The Supplier must ensure, and must ensure that all Sub-contractors and Computing Hubs ensure, that Authority Data is encrypted:
 - 6.1.1 when stored at any time when no operation is being performed on it; and
 - 6.1.2 when transmitted.
- 6.2 Where the Supplier, or a Sub-contractor, or a Computing Hub cannot encrypt Authority Data the Supplier must:
 - 6.2.1 immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - 6.2.2 provide details of the protective measures the Supplier or Sub-contractor (as applicable) or Computing Hub (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and
 - 6.2.3 provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.
- 6.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-contractor and Computing Hub shall meet to agree appropriate protective measures for the unencrypted Authority Data.
- 6.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
 - 6.4.1 the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

- 6.4.2 the protective measure that the Supplier, Sub-contractor and/or Computing Hub will put in place in respect of the unencrypted Authority Data.
- 6.5 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either party may refer the matter to be determined in accordance with the Dispute Resolution Procedure.
- 7 Patching and Vulnerability Scanning**
- 7.1 The Sub-contractor and Computing Hubs must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.
- 8 Third Party Sub-contractors**
- 8.1 The Sub-contractor and Computing Hubs must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.
- 8.2 The Sub-contractor and Computing Hubs must not, when performing any part of the Services, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Progress the Authority Data greater than those rights strictly necessary for the use of the software.

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE FOR PARTS A AND PART B

Security Management Plan Template

1 Executive Summary

2 System Description

2.1 Background

2.2 Organisational Ownership/Structure

- The solution will be holistically operated by STEM Learning Ltd and is portable to the Authority or other suppliers at contract termination or as otherwise requested in accordance with the contract.

2.3 Information assets and flows

2.4 System Architecture

2.5 Users

Locations

2.7 Test and Development Systems

2.8 Key roles and responsibilities

The roles that lead on security are:

- Departmental risk owners (the NCCE programme manager and Head of IT) - responsible for identifying risks related to information assets or systems

3 Risk Assessment

3.1 Accreditation/Assurance Scope

The scope of this assessment are the services documented in the high level system architecture paragraph above. It does not specifically cover the underlying infrastructure components of those services expect for where that infrastructure provides intrinsic assurances.

3.2 Risk appetite

3.3 Business impact assessment

--	--	--	--

3.4 Risk assessment

Risk ID	Inherent risk	Inherent level risk	Vulnerability	Controls	Residual risk level
R1	Internet attackers could gain unauthorised access	Medium	The service		Low
R2	Internal users may have copies of personal data	High			Low
R3	Internal user accounts may be compromised / misused	Medium		C5: Staff awareness training C7: Endpoint security	Low

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
----	---------------	---------------------	--

3.6 Residual risks and actions

4 In-service controls

5 Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

6 Major Hardware and Software and end of support dates

Name	Version	End of mainstream Sup- port/Extended Support	Notes/RAG Status
------	---------	---	------------------

Schedule 5 (Security Management)

- 7 Incident Management Process
- 8 Security Requirements for User Organisations
- 9 Required Changes Register

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
10	Sub-contractors					
	Annex A. ISO/IEC 27001 (at least ISO/IEC 27001:2013) and/or Cyber Essential Plus certificates					
	STEM Learning Cyber Essentials Plus Certificate - IASME-CEP-005670					
	Annex B. Cloud Security Principles assessment					
	Annex C. Protecting Bulk Data assessment if required by the Authority/Customer					
	Annex D. Latest ITHC report and Remediation Action Plan					

PART B: NOT USED

SCHEDULE 6

INSURANCE REQUIREMENTS

Schedule 6 (*Insurance Requirements*)

1 OBLIGATION TO MAINTAIN INSURANCES

- 1.1 Without prejudice to its obligations to the Authority under this Contract, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 and any other insurances as may be required by applicable Law (together the “**Insurances**”). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.
- 1.2 The 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.
- 1.3 The Insurances shall be taken out and maintained with insurers who are:
- (a) of good financial standing;
 - (b) appropriately regulated;
 - (c) regulated by the applicable regulatory body and is in good standing with that regulator; and
 - (d) except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.
- 1.4 The Supplier shall ensure that the public and products liability policy 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 Contract and for which the Supplier is legally liable.

2 GENERAL OBLIGATIONS

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
- (a) take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - (b) promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - (c) hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3 FAILURE TO INSURE

- 3.1 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 Insurances.
- 3.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the 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 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.

4 EVIDENCE OF INSURANCES

- 4.1 The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. 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.

5 CANCELLATION

- 5.1 Subject to Paragraph 5.2, the Supplier shall notify the Authority in writing at least 5 Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 5.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 5.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

6 INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

- 6.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Contract for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services and/or this Contract, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.
- 6.2 The Supplier shall maintain a register of all claims under the Insurances in connection with this Contract and shall allow the Authority to review such register at any time.
- 6.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 6.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Authority

Schedule 6 (Insurance Requirements)

any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX 1: REQUIRED INSURANCES

PART A: INSURANCE CLAIM NOTIFICATION

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within 20 Working Days after any insurance claim in excess of [REDACTED] relating to or arising out of the provision of the Services or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

PART B: THIRD PARTY PUBLIC AND PRODUCTS LIABILITY INSURANCE

- 1 Insured
 - 1.1 The Supplier
- 2 Interest
 - 2.1 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:
 - (a) death or bodily injury to or sickness, illness or disease contracted by any person; and
 - (b) loss of or damage to physical 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 and in connection with this Contract.
- 3 Limit of indemnity
 - 3.1 Not less than [REDACTED] in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period, but [REDACTED] in the aggregate per annum in respect of products and pollution liability.
- 4 Territorial limits

United Kingdom
- 5 Period of insurance
 - 5.1 From the date of this Contract for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing.
- 6 Cover features and extensions
 - 6.1 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 **Contract and for which the Supplier is legally liable.**

- 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 arising out of 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
 - 8.1 Not to exceed [REDACTED] for each and every third party property damage claim (personal injury claims to be paid in full).

PART C: UNITED KINGDOM COMPULSORY INSURANCES

- 1.1 The Supplier shall meet its insurance obligations under applicable Law in full, including, UK employers' liability insurance and motor third party liability insurance.
- 1.2 The limit of indemnity for the employers' liability insurance shall not be less than [REDACTED] [REDACTED] (or such other limit as may be required by Law from time to time) for any one occurrence inclusive of costs.
- 1.3 The employers' liability insurance shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority arising from the acts or omissions or the performance by the Supplier of the Services and in connection with this Contract.

PART D: ADDITIONAL INSURANCES

1. Professional Indemnity Insurance

1.1 Insured

The Supplier (the "**Insured**")

1.2 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 by reason of any negligent act, error and/or omission arising from or in connection with the provision of the Services and in connection with this Contract.

1.3 Limit of Indemnity

Not less than [REDACTED] in respect of any one claim and in the aggregate per annum.

1.4 Territorial Limits

United Kingdom

1.5 Period of Insurance

From the date of this Agreement for the duration of this Contract and renewable on an annual basis unless agreed otherwise and a period of three years (3) following the expiry date or the termination date whichever occurs earlier.

1.6 Cover Features and Extensions

Retroactive cover to apply to any claims made policy wording in respect of the Agreement or retroactive date to be no later than the date of this Contract.

1.7 Principal Exclusions

War and related perils

Nuclear and radioactive risks

1.8 Maximum Deductible

Not to exceed [REDACTED] for each and every claim

2 Cyber Liability Insurance

2.1 Insured

The Supplier (the "**Insured**")

2.2 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 by reason of any damage to, or loss of information from, IT systems and networks arising from or in connection with the provision of the Services and in connection with this Contract.

2.3 Limit of Indemnity

Cyber Plus - [REDACTED] [REDACTED]
in respect of any one claim and in the aggregate per annum

Public liability – [REDACTED] [REDACTED] in respect of any one claim and in the aggregate per annum.

2.4 Territorial Limits

United Kingdom

2.5 Period of Insurance

From the date of this Contract for the Term and renewable on an annual basis unless agreed otherwise and a period of three years (3) following the expiry date or the Termination Date whichever occurs earlier.

2.6 Cover Features and Extensions

Retroactive cover to apply to any claims made policy wording in respect of the Contract or retroactive date to be no later than the date of this Contract.

2.7 Principal Exclusions

War and related perils

Nuclear and radioactive risks

2.8 Maximum Deductible

[REDACTED] [REDACTED] for each and every claim

SCHEDULE 7

AUTHORITY RESPONSIBILITIES

Schedule 7 (*Authority Responsibilities*)

1 INTRODUCTION

- 1.1 The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Contract. Any obligations of the Authority in Schedule 2 (Services Description) and Schedule 8 (*Supplier Solution*) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be “Authority Responsibilities” and cross referenced in the table in Paragraph 3.
- 1.2 The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 GENERAL OBLIGATIONS

- 2.1 The Authority shall:
- (a) perform those obligations of the Authority which are set out in the Clauses of this Contract and the Paragraphs of the Schedules (except Schedule 2 (Services Description) and Schedule 8 (*Supplier Solution*));
 - (b) use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority’s staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;
 - (c) provide sufficient and suitably qualified staff to fulfil the Authority’s roles and duties under this Contract;
 - (d) use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Contract provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority; and

3 SPECIFIC OBLIGATIONS

- 3.1 The Authority shall, in relation to this Contract, perform the Authority's responsibilities identified as such in this Contract, the details of which are set out below:

Document	Location (Paragraph)	Authority responsibility
Document 3 (Statement of Requirements) of ITT pack	Function F, row F07	Communications approval and advice

Schedule 7 Authority Responsibilities)

		via Cabinet Office controls
Document 3 (Statement of Requirements) of ITT pack	Function D, row D1 and D1.1	Digital spend approval and advice via Cabinet Office controls
Document 2 of ITT pack Document 3 (Statement of Requirements) of ITT pack	Section 1.49, 1.50, 1.52, 1.55, 1.58, 1.60, 1.62 Function B, row B03.1	Approval of Grant Funding documentation prior to issue
Document 2 of ITT pack Document 3 (Statement of Requirements) of ITT pack	Section 1.41, 1.56, 1.57 Function B, row B02, B03, B06 and Function F, row F01.7	Approving of Grant Funding annually
Document 3 (Statement of Requirements) of ITT pack	Function F, row F01.1, F01.3, F01.5	Approval and review of documentation required by operational delivery and programme/contract management

SCHEDULE 8

SUPPLIER SOLUTION

The Supplier Solution is incorporated by reference and such documents(s) are detailed in the Virtual Library.

SCHEDULE 9
NOT USED

SCHEDULE 10

NOTIFIED KEY SUB-CONTRACTORS

Schedule 10 (Notified Key Sub-Contractors)

- 1 In accordance with Clause 15.11 (*Appointment of Key Sub-contractors*), the Supplier is entitled to sub-contract its obligations under this Contract to the Key Sub-contractors listed in the table below.
- 2 The Parties agree that they will update this Schedule periodically to record any Key Sub-contractors appointed by the Supplier with the consent of the Authority after the Effective Date for the purposes of the delivery of the Services.

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Term	Key role in delivery of the Services	Credit Threshold	Rating
					[Level 1]	

SCHEDULE 11

THIRD PARTY CONTRACTS

Schedule 11 (*Third Party Contracts*)

- 1 The contracts listed in the table below constitute Third Party Contracts entered into exclusively for the purposes of delivering the Services.
- 2 The Supplier shall be entitled to update this Schedule in accordance with Clause 15.5 (*Appointment of Sub-contractors*).
3. The Supplier will have updated this Schedule before the Operational Services Commencement Date. in accordance with Clause 15.5. The deadline for population is 28th February 2023 or other date as agreed between the Parties in writing.

Third party supplier name and address (if not the same as the registered office)	Registered office and company number	Related product/service description

SCHEDULE 12

SOFTWARE

Schedule 12 (Software)

1 THE SOFTWARE

- 1.1 The Software below is licensed to the Authority in accordance with Clause 16 (*Intellectual Property Rights*) and **Schedule 32 (Intellectual Property Rights)**.
- 1.2 The Parties agree that they will update this Schedule regularly, and in any event no less than every 6 (six) Months from the Effective Date, to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

2 SUPPLIER SOFTWARE

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
Teach Computing Website and Curriculum		Main NCCE site (teacher facing): course catalogue and booking; teacher resources	N/A	Future licenses to be for the sole purpose of National Centre for Computing Education delivery	1	Non-COTS	N/A
Impact Toolkit		Embed learning from CPD and evaluate impact	N/A	Future licenses to be for the sole purpose of National Centre for Computing Education delivery	1	Non-COTS	N/A
STEM Learning website		Teacher registration and course bookings	N/A	Future licenses to be for the sole purpose of National Centre for Computing	1	Non-COTS	N/A

Schedule 12 (Software)

				Education delivery			
Moodle		Online learning management system	N/A	N/A	1	Non-COTS	N/A
SQL Reporting		Build and populate data warehouse	N/A	Future licenses to be for the sole purpose of National Centre for Computing Education delivery	1	Non-COTS	N/A
Computing Quality Framework website						COTS	
Isaac Computer Science website						Non-COTS	

3 THIRD PARTY SOFTWARE

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/Expiry
Dynamics 365	████████	Back-end course/participant management system	1 license for each individual requiring access Currently ~300			COTS	Monthly license subscription
SmartModules/ SmartConnector	████████	Event management and integration tools for Dynamics	Annual support cost			COTS	Annual subscription
Logate for Dynamics	████████	Address geocoding tool	N/A			COTS	PAYG
Confluence	████████	Documentation repository	1 license for each individual requiring access Currently ~300			COTS	Monthly subscription

Schedule 12 (Software)

PowerBI		Reporting and BI for course/programme engagement and needs analysis	1 license for each individual requiring access Currently ~150			COTS	Monthly subscription
Azure data factory/SQL server		Provide data warehouse containers and ETL	1x ADFv2 instance 1x SQL DB S4			COTS	PAYG
Mailchimp (mandrill)		Transactional email from website registrations/bookings	N/A – licensed as a service			COTS	Monthly subscription
Community		Provide a community discussion area for participants				COTS	Annual License
Adestra		Upland software	Email marketing campaign tool			COTS	Annual License

ANNEX 1: FORM OF LETTER RE SUB-LICENSING OF SUPPLIER COTS SOFTWARE AND SUPPLIER COTS BACKGROUND IPRs

[Supplier letterhead]

[insert Authority

name and address]

[Date]

Dear Sirs

LICENCES FOR SUPPLIER COTS SOFTWARE AND SUPPLIER COTS BACKGROUND IPRs

We refer to the agreement between us dated *[insert date]* in respect of *[brief summary of subject of the Agreement]* (the “**Contract**”). Capitalised expressions used in this letter have the same meanings as in the Agreement.

In accordance with Paragraph [2.4(b) ***[use this if Options 1 or 2 in Schedule 32 (Intellectual Property Rights) are chosen]***] [2.5(b) ***[use this if Options 3 or 4 in Schedule 32 (Intellectual Property Rights) are used]***] of ***Schedule 32 (Intellectual Property Rights)*** of the Contract we confirm that:

- 1 the Authority is licensed by the Supplier to use the Supplier COTS Software and Supplier COTS Background IPRs identified in the first column of the Appendix to this letter (the “Appendix”) on the terms of the licences identified in the second column of the Appendix (the “Licences”); and
- 2 notwithstanding any provision to the contrary in the Licences, it is agreed that the Authority may sub-license, assign and novate the Supplier COTS Software and Supplier COTS Background IPRs as referred to in Paragraph [2.4(b) ***[use this if Options 1 or 2 in Schedule 32 (Intellectual Property Rights) are chosen]***] [2.5(b) ***[use this if Options 3 or 4 in Schedule 32 (Intellectual Property Rights) are used]***] of ***Schedule 32 (Intellectual Property Rights)*** of the Contract.

Yours faithfully

Signed:

On behalf of *[name of the Supplier]*

ANNEX 2: FORM OF CONFIDENTIALITY UNDERTAKING

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made on [*date*] 20

BETWEEN:

- (1) [*insert name*] of [*insert address*] (the “**Sub-licensee**”); and
- (2) [*insert name*] of [*insert address*] (the “**Supplier**” and together with the Supplier, the “**Parties**”).

WHEREAS:

- (A) [*insert name of Authority*] (the “**Authority**”) and the Supplier are party to a contract dated [*insert date*] (the “**Contract**”) for the provision by the Supplier of [*insert brief description of services*] to the Authority.
- (B) The Authority wishes to grant a sub-licence to the Sub-licensee in respect of certain software and intellectual property rights licensed to the Authority pursuant to the Contract (the “**Sub-licence**”).
- (C) It is a requirement of the Contract that, before the Authority grants such sub-licence to the Sub-licensee, the Sub-licensee execute a confidentiality agreement in favour of the Supplier in or substantially in the form of this Agreement to protect the Confidential Information of the Supplier.

IT IS AGREED as follows:

1 Interpretation

1.1 In this Agreement, unless the context otherwise requires:

“Confidential Information”

means:

- (a) Information, including all personal data within the meaning of the Data Protection Act 2018, and however it is conveyed, provided by the Authority to the Sub-licensee pursuant to or in connection with the Sub-licence that relates to:
 - (i) the Supplier; or
 - (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier;
- (b) the source code and the object code of the software sub-licensed to the Sub-licensee pursuant to the Sub-licence together with build information, relevant design and development information, technical specifications of all

functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation supplied by the Supplier to the Authority pursuant to or in connection with the Sub-licence;

(c) other Information provided by the Authority pursuant to this Agreement to the Sub-licensee that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Sub-licensee's attention or into the Sub-licensee's possession in connection with the Sub-licence; and

(d) Information derived from any of the above,

but not including any Information that:

(e) was in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the Authority;

(f) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or

(g) was independently developed without access to the Information;

“Information”

means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and

“Sub-licence”

has the meaning given to that expression in recital (B) to this Agreement.

1.2 In this Agreement:

(a) a reference to any gender includes a reference to other genders;

(b) the singular includes the plural and vice versa;

(c) the words “include” and cognate expressions shall be construed as if they were immediately followed by the words “without limitation”;

- (d) references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;
- (e) headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and
- (f) references to Clauses are to clauses of this Agreement.

2 Confidentiality Obligations

2.1 In consideration of the Authority entering into the Sub-licence, the Sub-licensee shall:

- (a) treat all Confidential Information as secret and confidential;
- (b) have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);
- (c) not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Supplier or except as expressly set out in this Agreement;
- (d) not transfer any of the Confidential Information outside the United Kingdom;
- (e) not use or exploit any of the Confidential Information for any purpose whatsoever other than as permitted under the Sub-licence;
- (f) immediately notify the Supplier in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and
- (g) upon the expiry or termination of the Sub-licence:
 - (i) destroy or return to the Supplier all documents and other tangible materials that contain any of the Confidential Information;
 - (ii) ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Sub-licensee) from any computer, word processor, voicemail system or any other device; and
 - (iii) make no further use of any Confidential Information.

3 Permitted Disclosures

- 3.1 The Sub-licensee may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:
- (a) reasonably need to receive the Confidential Information in connection with the Sub-licence; and
 - (b) have been informed by the Sub-licensee of the confidential nature of the Confidential Information; and
 - (c) have agreed to terms similar to those in this Agreement.
- 3.2 The Sub-licensee shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Sub-licensee.
- 3.3 Before making a disclosure pursuant to Clause 3.2, the Sub-licensee shall, if the circumstances permit:
- (a) notify the Supplier in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and
 - (b) ask the court or other public body to treat the Confidential Information as confidential.

4 General

- 4.1 The Sub-licensee acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Supplier shall remain with and be vested in the Supplier.
- 4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:
- (a) to grant the Sub-licensee any licence or rights other than as may be expressly stated in the Sub-licence;
 - (b) to require the Supplier to disclose, continue disclosing or update any Confidential Information; or
 - (c) as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of the Sub-licence.
- 4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.
- 4.4 Without prejudice to any other rights or remedies that the Supplier may have, the Sub-licensee acknowledges and agrees that damages alone may not be an

adequate remedy for any breach by the Sub-licensee of any of the provisions of this Agreement. Accordingly, the Sub-licensee acknowledges that the Supplier shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.

4.5 The maximum liability of the Sub-licensee to the Supplier for any breach of this Agreement shall be limited to [REDACTED]

4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.

4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.

4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5 Notices

5.1 Any notice to be given under this Agreement (each a “**Notice**”) shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.

5.2 Any Notice:

(a) if to be given to the Supplier shall be sent to:

[Address]

Attention: [Contact name and/or position, e.g. “The Finance Director”]

(b) if to be given to the Sub-licensee shall be sent to:

[Name of Organisation]

[Address]

Attention: []

6 Governing law

6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.

6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

IN WITNESS of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [*name of Supplier*]

Signature:

Date:

Name:

Position:

For and on behalf of [*name of Sub-licensee*]

Signature:

Date:

Name:

Position:

SCHEDULE 13

IMPLEMENTATION PLAN

Schedule 13 (*Implementation Plan*)

1 INTRODUCTION

1.1 This Schedule:

- (a) defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and
- (b) identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2 OUTLINE IMPLEMENTATION PLAN

2.1 The Outline Implementation Plan is set out in Annex 1.

2.2 All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 29 (*Authority Cause*)).

3 APPROVAL OF THE DETAILED IMPLEMENTATION PLAN

3.1 The Supplier shall submit a draft of the Detailed Implementation Plan to the Authority for approval within 20 Working Days of the Effective Date.

3.2 The Supplier shall ensure that the draft Detailed Implementation Plan:

- (a) incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan;
- (b) includes (as a minimum) the Supplier's proposed timescales in respect of the following for each of the Milestones:
 - (i) the completion of each design document;
 - (ii) the completion of the build phase;
 - (iii) the completion of any Testing to be undertaken in accordance with Schedule 14 (Testing Procedures); and
 - (iv) training and roll-out activities;
- (c) clearly outlines all the steps required to implement the Milestones to be achieved in the next 15 months, together with a high level plan for the rest of the programme, in conformity with the Authority Requirements;
- (d) clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and
- (e) is produced using a software tool as specified, or agreed by the Authority.

Schedule 13 (Implementation Plan)

- 3.3 Prior to the submission of the draft Detailed Implementation Plan to the Authority in accordance with Paragraph 3.1, the Authority shall have the right:
- (a) to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:
 - (i) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;
 - (ii) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and
 - (iii) any other work in progress in relation to the Detailed Implementation Plan; and
 - (b) to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.
- 3.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Authority shall:
- (a) review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and
 - (b) notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than 20 Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Authority.
- 3.5 If the Authority rejects the draft Detailed Implementation Plan:
- (a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and
 - (b) the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.
- 3.6 If the Authority approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Authority's notice of approval.
- 4 UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN**
- 4.1 Following the approval of the Detailed Implementation Plan by the Authority:
- (a) the Supplier shall submit a revised Detailed Implementation Plan to the Authority every 3 months starting 3 months from the Effective Date;

- (b) without prejudice to Paragraph 4.1(a), the Authority shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Authority within 20 Working Days of receiving such a request from the Authority (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);
 - (c) any revised Detailed Implementation Plan shall (subject to Paragraph 4.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 3; and
 - (d) the Supplier's performance against the Implementation Plan shall be monitored at meetings of the NCCE2 Steering Group (as defined in Schedule 21 (Governance). In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Authority not less than 5 Working Days in advance of each meeting of the Service Management Board.
- 4.2 Save for any amendments which are of a type identified and notified by the Authority (at the Authority's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:
 - (a) any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and
 - (b) in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 29 (*Authority Cause*).
- 4.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Authority.

5 GOVERNMENT REVIEWS

- 5.1 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

ANNEX 1: OUTLINE IMPLEMENTATION PLAN

The Implementation Plan is incorporated by reference and such documents(s) are detailed in the Virtual Library.

SCHEDULE 14
(TESTING PROCEDURES)

Schedule 14 (*Testing Procedures*)

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

“Component”	any constituent parts of the infrastructure for a Service, hardware or Software;
“Material Test Issue”	a Test Issue of Severity Level 1 or Severity Level 2;
“Severity Level”	the level of severity of a Test Issue, the criteria for which are described in Annex 1;
“Test Certificate”	a certificate materially in the form of the document contained in Annex 2 issued by the Authority when a Deliverable has satisfied its relevant Test Success Criteria;
“Test Issue”	any variance or non-conformity of a Deliverable from its requirements (such requirements being set out in the relevant Test Success Criteria);
“Test Issue Threshold”	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
“Test Issue Management Log”	a log for the recording of Test Issues as described further in Paragraph 9.1;
“Test Plan”	<p>a plan:</p> <ul style="list-style-type: none">(a) for the Testing of Deliverables; and(b) setting out other agreed criteria related to the achievement of Milestones, <p>as described further in Paragraph 5;</p>
“Test Reports”	the reports to be produced by the Supplier setting out the results of Tests;
“Test Specification”	the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 7;

“Test Strategy”	a strategy for the conduct of Testing as described further in Paragraph 4;
“Test Success Criteria”	in relation to a Test, the test success criteria for that Test as referred to in Paragraph 6;
“Test Witness”	any person appointed by the Authority pursuant to Paragraph 10.1; and
“Testing Procedures”	the applicable testing procedures and Test Success Criteria set out in this Schedule.

2 RISK

- 2.1 The issue of a Test Certificate, a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not:
- (a) operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Authority's requirements for that Deliverable or Milestone; or
 - (b) affect the Authority's right subsequently to reject:
 - (i) all or any element of the Deliverables to which a Test Certificate relates; or
 - (ii) any Milestone to which the Milestone Achievement Certificate relates.
- 2.2 Notwithstanding the issuing of any Milestone Achievement Certificate (including the Milestone Achievement Certificate in respect of Authority to Proceed), the Supplier shall remain solely responsible for ensuring that:
- (a) the Supplier Solution as designed and developed is suitable for the delivery of the Services and meets the Authority Requirements;
 - (b) the Services are implemented in accordance with this Contract; and
 - (c) each Target Performance Level is met from the relevant Operational Service Commencement Date.

3 TESTING OVERVIEW

- 3.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, the Test Plans and the Test Specifications.
- 3.2 The Supplier shall not submit any Deliverable for Testing:
- (a) unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;
 - (b) until the Authority has issued a Test Certificate in respect of any prior, dependant Deliverable(s); and

- (c) until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).
- 3.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable i.
- 3.4 Prior to the issue of a Test Certificate, the Authority shall be entitled to review the relevant Test Reports and the Test Issue Management Log.
- 3.5 Any Disputes between the Authority and the Supplier regarding Testing shall be referred to the Dispute Resolution Procedure using the Expedited Dispute Timetable.

4 TEST STRATEGY

- 4.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Effective Date but in any case no later than 20 Working Days (or such other period as the Parties may agree in writing) after the Effective Date.
- 4.2 The final Test Strategy shall include:
 - (a) an overview of how Testing will be conducted in accordance with the Implementation Plan;
 - (b) the process to be used to capture and record Test results and the categorisation of Test Issues;
 - (c) the method for mapping the expected Test results to the Test Success Criteria;
 - (d) the procedure to be followed if a Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issue©(e) the procedure to be followed to sign off each Test;
 - (e) the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for the resolution of Test Issues;
 - (f) the names and contact details of the Authority's and the Supplier's Test representatives;
 - (g) a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and Authority and/or third party involvement in the conduct of the Tests;
 - (h) the technical environments required to support the Tests; and
 - (i) the procedure for managing the configuration of the Test environments.

5 TEST PLANS

- 5.1 The Supplier shall develop Test Plans and submit these for the approval of the Authority as soon as practicable but in any case no later than 20 Working Days

(or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start date for the relevant Testing (as specified in the Implementation Plan).

5.2 Each Test Plan shall include as a minimum:

- (a) the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being tested and, for each Test, the specific Test Success Criteria to be satisfied;
- (b) a detailed procedure for the Tests to be carried out, including:
 - (i) the timetable for the Tests, including start and end dates;
 - (ii) the Testing mechanism;
 - (iii) dates and methods by which the Authority can inspect Test results or witness the Tests in order to establish that the Test Success Criteria have been met;
 - (iv) the mechanism for ensuring the quality, completeness and relevance of the Tests;
 - (v) the format and an example of Test progress reports and the process with which the Authority accesses daily Test schedules;
 - (vi) the process which the Authority will use to review Test Issues and the Supplier's progress in resolving these in a timely basis;
 - (vii) the Test Schedule;
 - (viii) the re-Test procedure, the timetable and the resources which would be required for re-Testing; and
- (c) the process for escalating Test Issues from a re-test situation to the taking of specific remedial action to resolve the Test Issue.

5.3 The Authority shall not unreasonably withhold or delay its approval of the Test Plans provided that the Supplier shall incorporate any reasonable requirements of the Authority in the Test Plans.

6 TEST SUCCESS CRITERIA

The Test Success Criteria for:

- (a) each Test that must be Achieved for the Supplier to Achieve either the ATP Milestone or a CPP Milestone are set out in Annex 4; and
- (b) all other Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 5.

7 TEST SPECIFICATION

7.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable

and in any event at least 10 Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start of the relevant Testing (as specified in the Implementation Plan).

7.2 Each Test Specification shall include as a minimum:

- (a) the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Authority and the extent to which it is equivalent to live operational data;
- (b) a plan to make the resources available for Testing;
- (c) Test scripts;
- (d) Test pre-requisites and the mechanism for measuring them; and
- (e) expected Test results, including:
 - (i) a mechanism to be used to capture and record Test results; and
 - (ii) a method to process the Test results to establish their content.

8 TESTING

8.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

8.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 10.

8.3 The Supplier shall notify the Authority at least 10 Working Days (or such other period as the Parties may agree in writing) in advance of the date, time and location of the relevant Tests and the Authority shall ensure that the Test Witnesses attend the Tests, except where the Authority has specified in writing that such attendance is not necessary.

8.4 The Authority may raise and close Test Issues during the Test witnessing process.

8.5 The Supplier shall provide to the Authority in relation to each Test:

- (a) a draft Test Report not less than 2 Working Days (or such other period as the Parties may agree in writing) prior to the date on which the Test is planned to end; and
- (b) the final Test Report within 5 Working Days (or such other period as the Parties may agree in writing) of completion of Testing.

8.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

- (a) an overview of the Testing conducted;

- (b) identification of the relevant Test Success Criteria that have been satisfied;
- (c) identification of the relevant Test Success Criteria that have not been satisfied together with the Supplier's explanation of why those criteria have not been met;
- (d) the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;
- (e) the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 9.1; and
- (f) the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

9 TEST ISSUES

- 9.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.
- 9.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Authority upon request.
- 9.3 The Authority shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

10 TEST WITNESSING

- 10.1 The Authority may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Authority, each of whom shall have appropriate skills to fulfil the role of a Test Witness.
- 10.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.
- 10.3 The Test Witnesses:
 - (a) shall actively review the Test documentation;
 - (b) will attend and engage in the performance of the Tests on behalf of the Authority so as to enable the Authority to gain an informed view of

whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

- (c) shall not be involved in the execution of any Test;
- (d) shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;
- (e) may produce and deliver their own, independent reports on Testing, which may be used by the Authority to assess whether the Tests have been Achieved;
- (f) may raise Test Issues on the Test Issue Management Log in respect of any Testing; and
- (g) may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

11 TEST QUALITY AUDIT

- 11.1 Without prejudice to its rights pursuant to Clause 12.2(b) (*Records, Reports, Audits & Open Book Data*), the Authority may perform on-going quality audits in respect of any part of the Testing (each a “**Testing Quality Audit**”) subject to the provisions set out in the agreed Quality Plan.
- 11.2 The focus of the Testing Quality Audits shall be on:
 - (a) adherence to an agreed methodology;
 - (b) adherence to the agreed Testing process;
 - (c) adherence to the Quality Plan;
 - (d) review of status and key development issues; and
 - (e) identification of key risk areas.
- 11.3 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.
- 11.4 The Authority will give the Supplier at least 5 Working Days' written notice of the Authority's intention to undertake a Testing Quality Audit and the Supplier may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Supplier's reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Authority will materially and adversely impact the Implementation Plan.
- 11.5 A Testing Quality Audit may involve document reviews, interviews with the Supplier Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule, the Authority witnessing Tests and demonstrations of the Deliverables to the Authority. Any Testing Quality Audit shall be limited in duration to a maximum time to be agreed between the Supplier and the Authority on a case by case basis (such agreement not to be unreasonably

withheld or delayed). The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Authority to enable it to carry out the Testing Quality Audit.

11.6 If the Testing Quality Audit gives the Authority concern in respect of the Testing Procedures or any Test, the Authority shall:

- (a) discuss the outcome of the Testing Quality Audit with the Supplier, giving the Supplier the opportunity to provide feedback in relation to specific activities; and
- (b) subsequently prepare a written report for the Supplier detailing its concerns,

and the Supplier shall, within a reasonable timeframe, respond in writing to the Authority's report.

11.7 In the event of an inadequate response to the Authority's report from the Supplier, the Authority (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate) until the issues in the report have been addressed to the reasonable satisfaction of the Authority.

12 OUTCOME OF TESTING

12.1 The Authority shall issue a Test Certificate as soon as reasonably practicable when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

2.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Authority shall notify the Supplier and:

- (a) the Authority may issue a Test Certificate conditional upon the remediation of the Test Issues;
- (b) where the Parties agree that there is sufficient time prior to the relevant Milestone Date, the Authority may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or
- (c) where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Authority's other rights and remedies, such failure shall constitute a Notifiable Default for the purposes of Clause 25.1 (*Rectification Plan Process*).

12.3 The Authority shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

3 ISSUE OF MILESTONE ACHIEVEMENT CERTIFICATE

- 3.1 The Authority shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:
- (a) the issuing by the Authority of Test Certificates and/or conditional Test Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and
 - (b) performance by the Supplier to the reasonable satisfaction of the Authority of any other tasks identified in the Implementation Plan as associated with that Milestone (which may include the submission of a Deliverable that is not due to be Tested, such as the production of Documentation).
- 3.2 The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 15 (Charges and Invoicing).
- 3.3 If a Milestone is not Achieved, the Authority shall promptly issue a report to the Supplier setting out:
- (a) the applicable Test Issues ; and
 - (b) any other reasons for the relevant Milestone not being Achieved.
- 3.4 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Authority shall issue a Milestone Achievement Certificate.
- 3.5 Without prejudice to the Authority's other remedies the following shall constitute a Notifiable Default for the purposes of Clause 25.1 (*Rectification Plan Process*) and the Authority shall refuse to issue a Milestone Achievement Certificate where:
- (a) there is one or more Material Test Issue(s); or
 - (b) the information required under Schedule 24 (*Reports and Records Provisions*) (Annex 3: *Records To Upload To Virtual Library*) has not been uploaded to the Virtual Library in accordance with Paragraph 3 of that Schedule.
- 3.6 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Authority may at its discretion (without waiving any rights in relation to the other options) choose to issue a Milestone Achievement Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:
- (a) any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Authority agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Authority within 10 Working Days of receipt of the Authority's report pursuant to Paragraph 13.3); and

Schedule 14 (Testing Procedures)

- (b) where the Authority issues a conditional Milestone Achievement Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

ANNEX 1: TEST ISSUES – SEVERITY LEVELS

- 1 Severity Level 1 Test Issue: a Test Issue that causes non-recoverable conditions, e.g. it is not possible to continue using a Component, a Component crashes, there is database or file corruption, or data loss;
- 2 Severity Level 2 Test Issue: a Test Issue for which, as reasonably determined by the Authority, there is no practicable workaround available, and which:
 - 2.1 causes a Component to become unusable;
 - 2.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or
 - 2.3 has an adverse impact on any other Component(s) or any other area of the Services;
- 3 Severity Level 3 Test Issue: a Test Issue which:
 - 3.1 causes a Component to become unusable;
 - 3.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or
 - 3.3 has an impact on any other Component(s) or any other area of the Services;
but for which, as reasonably determined by the Authority, there is a practicable workaround available;
- 4 Severity Level 4 Test Issue: a Test Issue which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Services; and
- 5 Severity Level 5 Test Issue: a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services

ANNEX 2: TEST CERTIFICATE

To: **[NAME OF SUPPLIER]**

FROM: **[NAME OF AUTHORITY]**

[Date]

Dear Sirs,

TEST CERTIFICATE

Deliverables: **[insert description of Deliverables]**

We refer to the agreement (the “**Contract**”) relating to the provision of the Services between the **[name of Authority]** (the “**Authority**”) and **[name of Supplier]** (the “**Supplier**”) dated **[date]**.

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (Definitions) or Schedule 14 (Testing Procedures) of the Contract.

[We confirm that the Deliverables listed above have been tested successfully in accordance with the Test Plan relevant to those Deliverables.]

OR

[This Test Certificate is issued pursuant to Paragraph 12.1 of Schedule 14 (Testing Procedures) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

**delete as appropriate*

Yours faithfully

[Name]

[Position]

acting on behalf of **[name of Authority]**

ANNEX 3: MILESTONE ACHIEVEMENT CERTIFICATE

To: **[NAME OF SUPPLIER]**

FROM: **[NAME OF AUTHORITY]**

[Date]

Dear Sirs,

MILESTONE ACHIEVEMENT CERTIFICATE

Milestone: **[insert description of Milestone]**

We refer to the agreement (the “**Contract**”) relating to the provision of the Services between the **[name of Authority]** (the “**Authority**”) and **[name of Supplier]** (the “**Supplier**”) dated **[date]**.

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (Definitions) or Schedule 14 (Testing Procedures) of the Contract.

[We confirm that all the Deliverables relating to Milestone **[number]** have been tested successfully in accordance with the Test Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]*

OR

[This Milestone Achievement Certificate is granted pursuant to Paragraph 13.1 of Schedule 14 (Testing Procedures) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Schedule 15 (Charges and Invoicing)]*

**delete as appropriate*

Yours faithfully

[Name]

[Position]

acting on behalf of **[Authority]**

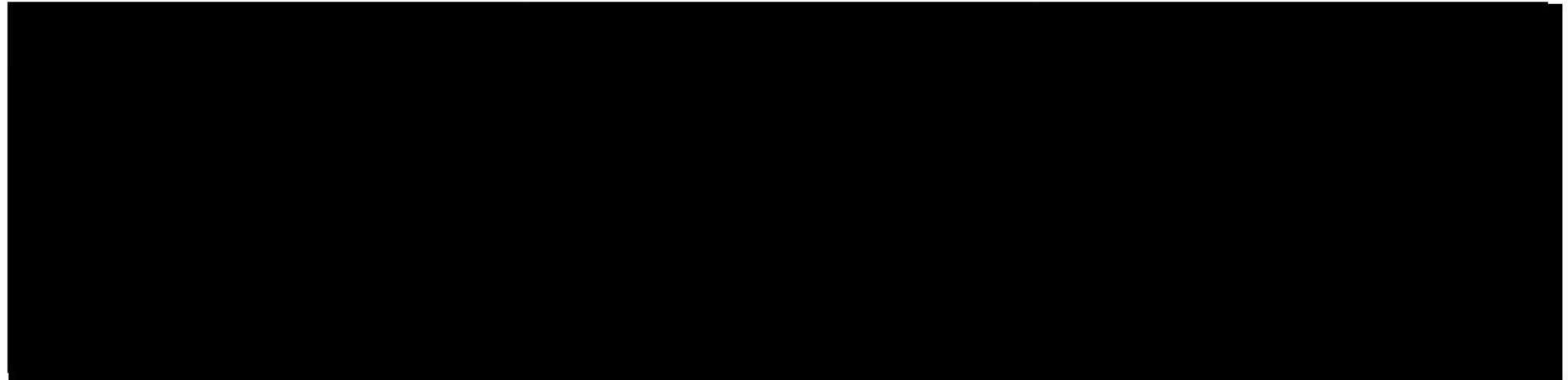
ANNEX 4: TEST SUCCESS CRITERIA

1 Tests to be Achieved in order to Achieve the ATP Milestone

Date	Description	Amount
2023-01-01	Opening Balance	1000.00
2023-01-05	Cash Sale	250.00
2023-01-10	Cash Sale	150.00
2023-01-15	Cash Sale	300.00
2023-01-20	Cash Sale	200.00
2023-01-25	Cash Sale	100.00
2023-01-30	Cash Sale	150.00
2023-02-05	Cash Sale	250.00
2023-02-10	Cash Sale	150.00
2023-02-15	Cash Sale	300.00
2023-02-20	Cash Sale	200.00
2023-02-25	Cash Sale	100.00
2023-02-28	Cash Sale	150.00
2023-03-05	Cash Sale	250.00
2023-03-10	Cash Sale	150.00
2023-03-15	Cash Sale	300.00
2023-03-20	Cash Sale	200.00
2023-03-25	Cash Sale	100.00
2023-03-30	Cash Sale	150.00
2023-04-05	Cash Sale	250.00
2023-04-10	Cash Sale	150.00
2023-04-15	Cash Sale	300.00
2023-04-20	Cash Sale	200.00
2023-04-25	Cash Sale	100.00
2023-04-30	Cash Sale	150.00
2023-05-05	Cash Sale	250.00
2023-05-10	Cash Sale	150.00
2023-05-15	Cash Sale	300.00
2023-05-20	Cash Sale	200.00
2023-05-25	Cash Sale	100.00
2023-05-30	Cash Sale	150.00
2023-06-05	Cash Sale	250.00
2023-06-10	Cash Sale	150.00
2023-06-15	Cash Sale	300.00
2023-06-20	Cash Sale	200.00
2023-06-25	Cash Sale	100.00
2023-06-30	Cash Sale	150.00
2023-07-05	Cash Sale	250.00
2023-07-10	Cash Sale	150.00
2023-07-15	Cash Sale	300.00
2023-07-20	Cash Sale	200.00
2023-07-25	Cash Sale	100.00
2023-07-30	Cash Sale	150.00
2023-08-05	Cash Sale	250.00
2023-08-10	Cash Sale	150.00
2023-08-15	Cash Sale	300.00
2023-08-20	Cash Sale	200.00

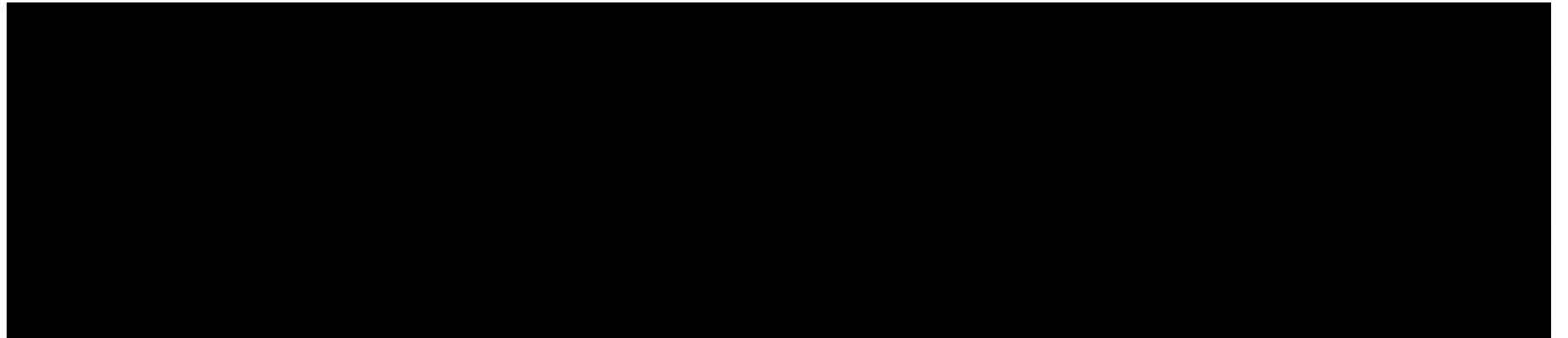
Date	Description	Amount	Balance
1/1/20	Opening Balance		0.00
1/5/20	Cash Sale	100.00	100.00
1/10/20	Cash Sale	250.00	350.00
1/15/20	Cash Sale	75.00	425.00
1/20/20	Cash Sale	125.00	550.00
1/25/20	Cash Sale	175.00	725.00
1/30/20	Cash Sale	225.00	950.00
2/5/20	Cash Sale	275.00	1225.00
2/10/20	Cash Sale	325.00	1550.00
2/15/20	Cash Sale	375.00	1925.00
2/20/20	Cash Sale	425.00	2350.00
2/25/20	Cash Sale	475.00	2825.00
2/30/20	Cash Sale	525.00	3350.00
3/5/20	Cash Sale	575.00	3925.00
3/10/20	Cash Sale	625.00	4550.00
3/15/20	Cash Sale	675.00	5225.00
3/20/20	Cash Sale	725.00	5950.00
3/25/20	Cash Sale	775.00	6725.00
3/30/20	Cash Sale	825.00	7550.00
3/31/20	Total Sales	7550.00	7550.00
4/1/20	Closing Balance		7550.00

This image is a scan of a blank white piece of paper. It contains no text, figures, or tables. There are a few small, dark specks scattered across the surface, which appear to be dust or scanning artifacts.



*** Note:** *The Pre-Conditions are that e.g. the Success Criteria for the previous Tests must be satisfied before the ATP Milestone tests are commenced*

2 Tests to be Achieved in order to Achieve a CPP Milestone



Schedule 14 (Testing Procedures)

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

SCHEDULE 15
(CHARGES AND INVOICING)

Schedule 15 (*Charges and Invoicing*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Certificate of Costs” a certificate of costs signed by the Supplier’s Chief Financial Officer or Director of Finance (or equivalent as agreed in writing by the Authority in advance of issue of the relevant certificate) and substantially in the format set out in Annex 3;

“The Employer Pension Contributions” means:

- (a) in respect of CSPA Eligible Employees those sums set out at Clauses 7.1.1 (*annual administration charges covering core services*), 7.1.5 (*employer contributions*), 7.1.7 (*the ASLC*) and 7.1.8 (*flat charges applicable to the Partnership Pension Account*) of the Admission Agreement;
- (b) in respect of NHSPA Eligible Employees, the standard employer contribution rate applicable to NHS Pension Scheme employers during the Term and payable by the Supplier (but no other costs, contributions, charges or surcharges payable by the Supplier to or in respect of the NHS Pension Scheme or in respect of any NHS Premature Retirement Rights, unless otherwise agreed in writing by the Authority);
- (c) in respect of LGPS Eligible Employees the standard employer contribution rate applicable to LGPS Eligible Employees during the Term and payable by the Supplier (but no other costs, contributions, charges or surcharges payable by the Supplier to or in respect of the LGPS or in respect of any Beckmann Liabilities, unless otherwise agreed in writing by the Authority); and

such other employer pension contributions, charges or costs incurred by the Supplier which have been expressly agreed by the Authority in writing to constitute 'Employer Pension Contributions';

“European Standard” in relation to an electronic invoice means the European standard and any of the syntaxes

	published in Commission Implementing Decision (EU) 2017/1870.
“Indexation” and “Index”	the adjustment of an amount or sum in accordance with Retail Prices Index, Consumer Prices Index or Average Earnings Index;
“Overhead”	those amounts which are intended to recover a proportion of the Supplier’s or the Key Sub-contractor’s (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Personnel and accordingly included within limb (a) of the definition of “Costs”;
“Supporting Documentation”	sufficient information in writing to enable the Authority reasonably to assess whether the Charges, Milestone Payments and other sums due from the Authority detailed in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts;
“Work Day”	7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
“Work Hours”	the hours spent by the Supplier Personnel properly working on the Services including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;

PART A: PRICING

1 APPLICABLE PRICING MECHANISM

- 1.1 Implementation Milestone Payments and Service Charges shall be calculated using the pricing mechanism specified in Annex 1 as more particularly set out in this Schedule.
- 1.2 KPI Milestone Payments shall be calculated in accordance with the KPI Milestone Payment threshold as set out in Annex 1 of Schedule 3 (Performance Levels). The maximum KPI Milestone Payment due to the Supplier is as set out in Table 2 of Annex 1 of this Schedule.
- 1.3 Tables 1 and 2 of Annex 1 to this Schedule sets out that the “Firm Price” pricing mechanism shall be used to calculate each Milestone Payment, and Paragraph 5 shall apply.
- 1.4 Table 3 of Annex 1 to this Schedule sets out that the “Firm Price” pricing mechanism shall be used to calculate each Service Charge, and Paragraph 4 shall apply.

2 NOT USED

3 NOT USED

4 FIRM PRICE SERVICE CHARGES

- 4.1 Where Service Charge is to be calculated by reference to a Firm Price pricing mechanism, the relevant Charge shall be the amount set out against that Charge in Table 3 of Annex 1.
- 4.2 Charges calculated by reference to a Firm Price pricing mechanism shall not be subject to increase by way of Indexation.

5 FIRM PRICE MILESTONE PAYMENTS

- 5.1 Where a Milestone Payment is to be calculated by reference to a Firm Price pricing mechanism, the relevant Charge shall be the amount set out against that Charge in Tables 1 and 2 of Annex 1.
- 5.2 Table 1 sets out the maximum Implementation Milestone Payments and Table 2 sets out the maximum KPI Milestone Payments.
- 5.3 Charges calculated by reference to a Firm Price pricing mechanism shall not be subject to increase by way of Indexation.

6. GRANT FUNDING AND INCENTIVE PAYMENTS

- 6.1 The Authority will pay the Supplier any Grant Funding payments and Incentive Payments (as applicable) in accordance with the provisions of Schedule 33 (Grant Funding and Incentive Payments).

PART B: CHARGING MECHANISMS

1 MILESTONE PAYMENTS

- 1.1 Subject to the Achievement of a Milestone the Supplier shall be entitled to invoice the Authority for the Milestone Payment associated with that Milestone.
- 1.2 Each invoice relating to a Milestone Payment shall be supported by a Milestone Achievement Certificate and Certificate of Costs with Supporting Documentation.

2 SERVICE CHARGES

- 2.1 Service Charges shall be invoiced by the Supplier for each Service Period in arrears in accordance with the requirements of Part D.
- 2.2 Any Service Credits that accrue during a Service Period shall be deducted from the Service Charges payable in accordance with Part C of this Schedule. An invoice for a Service Charge shall not be payable by the Authority unless all adjustments (including Service Credits) relating to the Service Charges for the immediately preceding Service Period have been agreed.

PART C: ADJUSTMENTS TO THE CHARGES AND RISK REGISTER

1 DELAY PAYMENTS

- 1.1 If a Key Milestone has not been Achieved on or before the relevant Milestone Date, the Supplier shall pay a Delay Payment to the Authority in respect of that Key Milestone. Delay Payments shall accrue:
- (a) at the daily rate (the “**Delay Payment Rate**”) determined in accordance with Paragraph 1.2;
 - (b) from (but excluding) the relevant Milestone Date to (and including) the later of:
 - (i) the date on which the Key Milestone is Achieved; and
 - (ii) the expiry of the Delay Deduction Period; and
 - (c) on a daily basis, with any part day’s Delay counting as a day.
- 1.2 Where a Delay Payment is payable in respect of a Key Milestone, the Delay Payment Rate shall be:
- (a) where the Supplier has given the Authority less than 3 months’ prior notice of the Delay, the amount set out in column 4 of Table 1 of Annex 2 for the Key Milestone;
 - (b) where the Supplier has given the Authority between three (3) months’ and six (6) months’ prior notice of the Delay, the amount set out in column 5 of Table 1 of Annex 2 for the Key Milestone; or
 - (c) where the Supplier has given the Authority more than 6 months’ prior notice of the Delay, the amount set out in column 6 of Table 1 of Annex 2 for the Key Milestone.
- 1.3 Where the Supplier serves a notice pursuant to Paragraph 1.2(b) or 1.2(c), the Supplier shall, within 5 Working Days of the date the notice is served:
- (a) pay to the Authority in cleared funds on account of the relevant Delay Payment (but subject always to Paragraph 1.4) an amount equal to:
 - (i) in the case of a notice served pursuant to Paragraph 1.2(b), five (5) days of Delay Payments; or
 - (ii) in the case of a notice served pursuant to Paragraph 1.2(c), ten (10) days of Delay Payments in accordance with Paragraph 1.4,in each case calculated at the applicable Delay Payment Rate; and
 - (b) issue a credit note to the Authority in respect of the relevant amount.
- Failure to make payment within 10 Working Days of the Supplier’s notice shall invalidate the notice.

- 1.4 Any amounts paid to the Authority pursuant to Paragraph 1.3 shall not be refundable to the Supplier in any circumstances, including where a Delay as referred to in the Supplier's notice:
- (a) does not occur; or
 - (b) does occur but continues for fewer days during the relevant Delay Deduction Period than the number of days referred to in Paragraph 1.3(a) or 1.3(b) as the case may be.
- 1.5 The Parties agree that Delay Payments calculated in accordance with the applicable Delay Payment Rates are in each case a genuine pre-estimate of the Losses which the Authority will incur as a result of any failure by the Supplier to Achieve the relevant Key Milestone by the Milestone Date. Delay Payment Rates are stated exclusive of VAT.
- 1.6 The Delay Payment in respect of a Key Milestone (net of any payment made in respect of that Key Milestone pursuant to Paragraph 1.3) shall be shown as a deduction from the amount due from the Authority to the Supplier in the next invoice due to be issued by the Supplier after the date on which the relevant Key Milestone is Achieved or the expiry of the Delay Deduction Period (as the case may be). If the relevant Key Milestone is not Achieved by the expiry of the Delay Deduction Period and no invoice is due to be issued by the Supplier within 10 Working Days of expiry of the Delay Deduction Period, then the Supplier shall within 10 Working Days of expiry of the Delay Deduction Period:
- (a) issue a credit note to the Authority in respect of the total amount of the Delay Payment in respect of the Key Milestone (net of any payment made in respect of the Key Milestone pursuant to Paragraph 1.3); and
 - (b) pay to the Authority as a debt a sum equal to the total amount of the Delay Payment in respect of the Key Milestone together with interest on such amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from (and including) the due date up to (but excluding) the date of actual payment, whether before or after judgment.

2 PAYMENTS FOR DELAYS DUE TO AUTHORITY CAUSE

- 2.1 If the Supplier is entitled in accordance with Clause 29.1(iii)(D) (*Authority Cause*) to compensation for failure to Achieve an Implementation Milestone by its Milestone Date, then, subject always to Clause 23 (*Limitations on Liability*), such compensation shall be determined in accordance with the following principles:
- (a) the compensation shall reimburse the Supplier for additional costs incurred by the Supplier that the Supplier:
 - (i) can demonstrate it has incurred solely and directly as a result of the Authority Cause; and
 - (ii) is, has been, or will be unable to mitigate, having complied with its obligations under Clause 29.1 (*Authority Cause*);

Schedule 15 (Charges and Invoicing)

- (b) the compensation shall not operate so as to put the Supplier in a better position than it would have been in but for the occurrence of the Authority Cause; and
- (c) where the relevant Milestone Payment is to be calculated based upon a Firm Price pricing mechanism, the compensation shall include such amount as is set out in respect of the relevant Milestone in Table 1 of Annex 1.

2.2 The Supplier shall provide the Authority with any information the Authority may require in order to assess the validity of the Supplier's claim to compensation.

3. SERVICE CREDITS

3.1 Service Credits shall be calculated by reference to the number of Service Points accrued in any one Service Period pursuant to the following:

3.2 For each Service Period:

- (a) the total Service Credits applicable for the Service Period shall be calculated in accordance with the following formula:

$$SC = TSP \times \blacksquare$$

where:

SC is the total Service Credits for the relevant Service Period;

TSP is the total Service Points that have accrued for the relevant Service Period;

- 3.3 The maximum Service Points that can be accrued per Service Period are two (2), and therefore the maximum Service Points that can be accrued annually is twenty-four (24).
- 3.4 Service Credits are a reduction of the Service Charges payable in respect of the relevant Services to reflect the reduced value of the Services actually received and are stated exclusive of VAT. The Service Credits deducted from the Service Charges shall not exceed the Service Credit Cap.
- 3.5 At 6 Month intervals Service Credits shall be shown as a deduction from the amount due from the Authority to the Supplier totalled and applied to that Month's invoice; this will be referred to as the 'Service Credit'. At the expiry or earlier termination of the Contract they will be applied to the final invoice if this does not land on a 6-Monthly interval, on a pro rata basis.

4. CHANGES TO CHARGES

- 4.1 Any Changes to the Charges shall be developed and agreed by the Parties in accordance with [Schedule 22 \(Change Control Procedure\)](#)
- 4.2 The Authority may request that any Impact Assessment presents Charges without Indexation for the purposes of comparison.

5. RISK REGISTER

- 5.1 The Parties shall review the Risk Register in the Virtual Library from time to time and as otherwise required for the purposes of Schedule 24 (Reports and Records Provisions).

PART D: INVOICING AND PAYMENT TERMS

1 SUPPLIER INVOICES

- 1.1 The Authority shall accept for processing any electronic invoice that complies with the European Standard, provided that it is valid and undisputed.
- 1.2 If the Supplier proposes to submit for payment an invoice that does not comply with the European Standard the Supplier shall:
 - (a) comply with the requirements of the Authority's e-invoicing system;
 - (b) prepare and provide to the Authority for approval of the format a template invoice within 10 Working Days of the Effective Date which shall include, as a minimum the details set out in Paragraph 1.3 together with such other information as the Authority may reasonably require to assess whether the Charges that will be detailed therein are properly payable; and
 - (c) make such amendments as may be reasonably required by the Authority if the template invoice outlined in (b) is not approved by the Authority.
- 1.3 The Supplier shall ensure that each invoice is submitted in the correct format for the Authority's e-invoicing system, or that it contains the following information:
 - (a) the date of the invoice;
 - (b) a unique invoice number;
 - (c) the Service Period or other period(s) to which the relevant Charge(s) relate;
 - (d) the correct reference for this Contract;
 - (e) the reference number of the purchase order to which it relates (if any);
 - (f) the dates between which the Services subject of each of the Charges detailed on the invoice were performed;
 - (g) a description of the Services;
 - (h) the pricing mechanism used to calculate the Charges;
 - (i) any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;
 - (j) the total Charges gross and net of any applicable deductions and, separately, chargeable to the Authority under the terms of this Contract, and, separately, any VAT or other sales tax payable in respect of each of the same;
 - (k) details of any Service Credits similar deductions that shall apply to the Charges detailed on the invoice;

Schedule 15 (Charges and Invoicing)

- (l) reference to any reports required by the Authority in respect of the Services to which the Charges detailed on the invoice relate (or in the case of reports issued by the Supplier for validation by the Authority, then to any such reports as are validated by the Authority in respect of the Services);
 - (m) a contact name and telephone number of a responsible person in the Supplier's finance department in the event of administrative queries;
 - (n) the banking details for payment to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number); and
 - (o) where the Services have been structured into separate Service lines, the information at (a) to (n) of this Paragraph 1.3 shall be broken down in each invoice per Service line.
- 1.4 The Supplier shall invoice the Authority in respect of Services in accordance with the requirements of Part B. The Supplier shall first submit to the Authority a draft invoice setting out the Charges payable and Milestone Payments. The Parties shall endeavour to agree the draft invoice within 5 Working Days of its receipt by the Authority, following which the Supplier shall be entitled to submit its invoice. In relation to the Service Charges the Supplier shall invoice the Authority per Service Period up to a maximum of the amounts set out in Table 3 of Annex 1.
- 1.5 Each invoice shall at all times be accompanied by Supporting Documentation. Any assessment by the Authority as to what constitutes Supporting Documentation shall not be conclusive and the Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.
- 1.6 The Supplier shall submit all invoices and Supporting Documentation to AccountsPayable.OCR@education.gov.uk with a copy (again including any Supporting Documentation) to such other person and at such place as the Authority may notify to the Supplier from time to time.
- 1.7 All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.
- 1.8 The Authority shall regard an invoice as valid only if it complies with the provisions of this Part D. Where any invoice does not conform to the Authority's requirements set out in this Part D, the Authority shall promptly return the disputed invoice to the Supplier and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.
- 1.9 If the Authority fails to consider and verify an invoice in accordance with Paragraphs 1.4 and 1.8, the invoice shall be regarded as valid and undisputed for the purpose of Paragraph 2.1 30 days after a reasonable time has passed.

2 PAYMENT TERMS

- 2.1 Subject to the relevant provisions of this Schedule, the Authority shall make payment to the Supplier within thirty (30) days of verifying that the invoice is valid and undisputed.
- 2.2 Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice.

ANNEX 1: PRICING MECHANISM

TABLE 1: IMPLEMENTATION MILESTONE PAYMENTS

Charge Number	Milestone	Pricing Mechanism	Maximum Payment	Milestone Date	Payment Date
44		FIRM			
45		FIRM			
46		FIRM			
47		FIRM			
48		FIRM			
49		FIRM			
50		FIRM			
51		FIRM			

TABLE 2: KPI MILESTONE PAYMENTS

Charge Number	Key Performance Indicator	Pricing Mechanism	Maximum Payment	Milestone Date	Payment Date
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					
34					
35					
36					
37					
38					
39					
40					
41					
42					
43					
44					
45					
46					
47					
48					
49					
50					
51					
52					
53					
54					
55					
56					
57					
58					
59					
60					
61					
62					
63					
64					
65					
66					
67					
68					
69					
70					
71					
72					
73					
74					
75					
76					
77					
78					
79					
80					
81					
82					
83					
84					
85					
86					
87					
88					
89					
90					
91					
92					
93					
94					
95					
96					
97					
98					
99					
100					

TABLE 3: SERVICE CHARGES

Charge Number	Payment Mechanism	Date	Payment
15	FIRM		
16	FIRM		
17	FIRM		
18	FIRM		
19	FIRM		
20	FIRM		
21	FIRM		
22	FIRM		
23	FIRM		
24	FIRM		
25	FIRM		
26	FIRM		
27	FIRM		
28	FIRM		
29	FIRM		
30	FIRM		
31	FIRM		
32	FIRM		
33	FIRM		

Schedule 15 (Charges and Invoicing)

Charge Number	Payment Mechanism	Date	Payment
34	FIRM		
35	FIRM		
36	FIRM		
37	FIRM		
38	FIRM		
39	FIRM		
40	FIRM		
41	FIRM		
42	FIRM		
43	FIRM		

ANNEX 2: NOT USED

ANNEX 3: PRO-FORMA CERTIFICATE OF COSTS

I **[name of CFO or Director of Finance or equivalent as agreed in advance in writing with the Authority]** of **[insert name of Supplier]**, certify that the financial information provided as part of this Certificate of Costs, incurred in relation to the **[insert name/reference for the Contract]** (the “**Contract**”) in relation to the following [Milestone]:

[Insert details of Milestone]

- 1** has been reasonably and properly incurred in accordance with **[name of Supplier]**'s books, accounts, other documents and records;
- 2** is accurate and not misleading in all key respects; and
- 3** is in conformity with the Contract and with all generally accepted accounting principles within the United Kingdom.

Signed **[Director of Finance or equivalent]**

[Name of Supplier]

ANNEX 4: NOT USED

SCHEDULE 16

PAYMENTS ON TERMINATION

Schedule 16 (*Payments on Termination*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Applicable Supplier Personnel”

any Supplier Personnel who:

(a) at the Termination Date:

- (i) are employees of the Supplier;
- (ii) are Dedicated Supplier Personnel;
- (iii) have not transferred (and are not in scope to transfer at a later date) to the Authority or the Replacement Supplier by virtue of the Employment Regulations; and

(b) are dismissed or given notice of dismissal by the Supplier within:

- (i) 40 Working Days of the Termination Date; or
- (ii) such longer period required by Law, their employment contract (as at the Termination Date) or an applicable collective agreement; and

(c) have not resigned or given notice of resignation prior to the date of their dismissal by the Supplier; and

(d) the Supplier can demonstrate to the satisfaction of the Authority:

- (i) are surplus to the Supplier's requirements after the Termination Date notwithstanding its obligation to provide services to its other customers;
- (ii) are genuinely being dismissed for reasons of redundancy; and
- (iii) have been selected for redundancy by the Supplier on objective grounds other than the fact that the Supplier is entitled to reimbursement under this provision in respect of such employees;

“Breakage Costs Payment”	an amount equal to the Redundancy Costs and the Contract Breakage Costs as at the Termination Date as determined in accordance with Paragraph 3;
“Contract Breakage Costs”	the amounts payable by the Supplier to its Key Sub-contractors or other third parties (as applicable) for terminating all relevant Key Sub-contracts or Third Party Contracts as a direct result of the early no-fault termination of this Contract;
“Dedicated Supplier Personnel”	all Supplier Personnel then assigned to the Services or any part of the Services. If the Supplier is unsure as to whether Supplier Personnel are or should be regarded as so assigned, it shall consult with the Authority whose view shall be determinative provided that the employee has been materially involved in the provision of the Services or any part of the Services;
“Redundancy Costs”	<p>the total sum of any of the following sums paid to Applicable Supplier Personnel, each amount apportioned between the Supplier and the Authority based on the time spent by such employee on the Services as a proportion of the total Service duration:</p> <ul style="list-style-type: none">(a) any statutory redundancy payment; and(b) in respect of an employee who was a Transferring Former Supplier Employee or a Transferring Authority Employee, any contractual redundancy payment (or where such a contractual benefit on redundancy is a benefit payable from a pension scheme, the increase in cost to the Supplier as a net present value compared to the benefit payable on termination of employment without redundancy), provided that such employee was entitled to such contractual redundancy payment immediately prior to his or her transfer to the Supplier under the Employment Regulations;
“Request for Estimate”	a written request sent by the Authority to the Supplier, requiring that the Supplier provide it with an accurate estimate of the Termination Payment and Compensation Payment that would be payable if the Authority exercised its right under Clause 31.1(a) (<i>Termination by the Authority</i>) to terminate

this Contract for convenience on a specified Termination Date;

“Shortfall Period” has the meaning given in Paragraph 6.2;

“Termination Estimate” has the meaning given in Paragraph 11.2:

“Third Party Contract” a contract with a third party entered into by the Supplier exclusively for the purpose of delivering the Services, as listed in Schedule 11 (Third Party Contracts));

2 TERMINATION PAYMENT

- 2.1 The Termination Payment payable pursuant to Clause 32.3(a) (*Payments by the Authority*) shall be an amount equal to the Breakage Costs Payment.

3 BREAKAGE COSTS PAYMENT

- 3.1 The Supplier may recover through the Breakage Costs Payment only those costs incurred by the Supplier directly as a result of the termination of this Contract which:
- (a) would not have been incurred had this Contract continued until expiry of the Initial Term, or in the event that the Term has been extended, the expiry of the Extension Period;
 - (b) are unavoidable, proven, reasonable, and not capable of recovery;
 - (c) are incurred under arrangements or agreements that are directly associated with this Contract;
 - (d) are not Contract Breakage Costs relating to contracts or Sub-contracts with Affiliates of the Supplier; and
 - (e) relate directly to the termination of the Services.

Limitation on Breakage Costs Payment

- 3.2 The Breakage Costs Payment shall not exceed 120% of the preceding three (3) months Charges, calculated at the point a Termination Estimate is requested in accordance with paragraph 11.

Redundancy Costs

- 3.3 The Authority shall not be liable under this Schedule for any costs associated with Supplier Personnel (whether relating to redundancy, redeployment or otherwise) other than the Redundancy Costs.
- 3.4 Where the Supplier can demonstrate that a member of Supplier Personnel will be made redundant following termination of this Contract, but redeployment of such person is possible and would offer value for money to the Authority when compared with redundancy, then the Authority shall pay the Supplier the actual

direct costs incurred by the Supplier or its Sub-contractor arising out of the redeployment of such person (including retraining and relocation costs) subject to a maximum amount of [REDACTED] per relevant member of the Supplier Personnel.

Contract Breakage Costs

- 3.5 The Supplier shall be entitled to Contract Breakage Costs only in respect of Third Party Contracts or Sub-contracts which:
- (a) are not assigned or novated to a Replacement Supplier at the request of the Authority in accordance with Schedule 25 (Exit Management); and
 - (b) the Supplier can demonstrate:
 - (i) are surplus to the Supplier's requirements after the Termination Date, whether in relation to use internally within its business or in providing services to any of its other customers; and
 - (ii) have been entered into by it in the ordinary course of business.
- 3.6 The Supplier shall seek to negotiate termination of any Third Party Contracts or Sub-contracts with the relevant third party or Sub-contractor (as the case may be) using all reasonable endeavours to minimise the cancellation or termination charges.
- 3.7 Except with the prior written agreement of the Authority, the Authority shall not be liable for any costs (including cancellation or termination charges) that the Supplier is obliged to pay in respect of:
- (a) the termination of any contractual arrangements for occupation of, support of and/or services provided for Supplier premises which may arise as a consequence of the termination of this Contract; and/or
 - (b) Assets not yet installed at the Termination Date.

4 NOT USED

5 MITIGATION OF CONTRACT BREAKAGE COSTS AND REDUNDANCY COSTS

- 5.1 The Supplier agrees to use all reasonable endeavours to minimise and mitigate Contract Breakage Costs and Redundancy Costs by:
- (a) the appropriation of Assets, employees and resources for other purposes;
 - (b) at the Authority's request, assigning any Third Party Contracts and Sub-contracts to the Authority or a third party acting on behalf of the Authority; and
 - (c) in relation Third Party Contracts and Sub-contract that are not to be assigned to the Authority or to another third party, terminating those

contracts at the earliest possible date without breach or where contractually permitted.

- 5.2 If Assets, employees and resources can be used by the Supplier for other purposes, then there shall be an equitable reduction in the Contract Breakage Costs and Redundancy Costs payable by the Authority or a third party to the Supplier. In the event of any Dispute arising over whether the Supplier can use any Assets, employees and/or resources for other purposes and/or over the amount of the relevant equitable reduction, the Dispute shall be referred to an Expert for determination in accordance with the procedure detailed in Schedule 23 (Dispute Resolution Procedure).

6 NOT USED

- 6.1 Not Used

7 FULL AND FINAL SETTLEMENT

- 7.1 Any Termination Payment paid under this Schedule shall be in full and final settlement of any claim, demand and/or proceedings of the Supplier in relation to any termination by the Authority pursuant to Clause 31.1(a) (*Termination by the Authority*) or termination by the Supplier pursuant to Clause 31.3(a) (*Termination by the Supplier*) (as applicable), and the Supplier shall be excluded from all other rights and remedies it would otherwise have been entitled to in respect of any such termination.

8 INVOICING FOR THE PAYMENTS ON TERMINATION

- 8.1 All sums due under this Schedule shall be payable by the Authority to the Supplier in accordance with the invoicing and payment terms set out in Part D of Schedule 15 (Charges and Invoicing).

9 SET OFF

- 9.1 The Authority shall be entitled to set off any outstanding liabilities of the Supplier against any amounts that are payable by it pursuant to this Schedule.

10 NO DOUBLE RECOVERY

- 10.1 If any amount payable under this Schedule (in whole or in part) relates to or arises from any Transferring Assets then, to the extent that the Authority makes any payments pursuant to Schedule 25 (Exit Management) in respect of such Transferring Assets, such payments shall be deducted from the amount payable pursuant to this Schedule.
- 10.2 The value of the Termination Payment shall be reduced or extinguished to the extent that the Supplier has already received the Charges or the financial benefit of any other rights or remedy given under this Contract so that there is no double counting in calculating the relevant payment.
- 10.3 Any payments that are due in respect of the Transferring Assets shall be calculated in accordance with the provisions of the Exit Plan.

11 ESTIMATE OF TERMINATION PAYMENT

- 11.1 The Authority may issue a Request for Estimate at any time during the Term provided that no more than 2 Requests for Estimate may be issued in any 6 month period.
- 11.2 The Supplier shall within 20 Working Days of receiving the Request for Estimate (or such other timescale agreed between the Parties), provide an accurate written estimate of the Termination Payment that would be payable by the Authority based on a postulated Termination Date specified in the Request for Estimate (such estimate being the “**Termination Estimate**”). The Termination Estimate shall:
- (a) be based on the relevant amounts set out in Schedule 15 (Charges and Invoicing);;
 - (b) include:
 - (i) details of the mechanism by which the Termination Payment is calculated;
 - (ii) full particulars of the estimated Contract Breakage Costs in respect of each Sub-contract or Third Party Contract and appropriate supporting documentation; and
 - (iii) such information as the Authority may reasonably require; and
 - (c) state the period for which that Termination Estimate remains valid, which shall be not less than 20 Working Days.
- 11.3 The Supplier acknowledges that issue of a Request for Estimate shall not be construed in any way as to represent an intention by the Authority to terminate this Contract.
- 11.4 If the Authority issues a Termination Notice to the Supplier within the stated period for which a Termination Estimate remains valid, the Supplier shall use the same mechanism to calculate the Termination Payment as was detailed in the Termination Estimate unless otherwise agreed in writing between the Supplier and the Authority.

ANNEX 1: MAXIMUM PAYMENTS ON TERMINATION – Not Applicable

SCHEDULE 17
NOT USED

SCHEDULE 18

FINANCIAL DISTRESS

Schedule 18 (*Financial Distress*)

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

“Board”	means the Supplier’s board of directors;
“Board Confirmation”	means written confirmation from the Board in accordance with Paragraph 8 of this Schedule;
“FDE Group”	means the Supplier, Key Sub-contractors, and the Monitored Suppliers;
“Financial Indicators”	in respect of the Supplier, Key Sub-contractors, means each of the financial indicators set out at Paragraph 5.1 of this Schedule;;
“Financial Target Thresholds”	means the target thresholds for each of the Financial Indicators set out at Paragraph 5.1 of this Schedule;

2 WARRANTIES AND DUTY TO NOTIFY

2.1 The Supplier warrants and represents to the Authority for the benefit of the Authority that as at the Effective Date the financial position or, as appropriate, the financial performance of each of the Supplier, and Key Sub-contractors satisfies the Financial Target Thresholds.

2.2 The Supplier shall:

- (a) monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least at the frequency set out for each at Paragraph 5.1 (where specified) and in any event, on a regular basis and no less than once a year within one hundred and twenty (120) days after the Accounting Reference Date; and
- (b) promptly notify (or shall procure that its auditors promptly notify) the Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event). Any fact, circumstance or matter which could cause a Financial Distress Event might include but not be limited to where any FDE Group entity intends to reduce the number of personnel assigned to the delivery of the Services by 10% or more.

2.3 Each report submitted by the Supplier pursuant to Paragraph 2.2 shall:

- (a) be a single report with separate sections for each of the FDE Group entities;
- (b) contain a sufficient level of information to enable the Authority to verify the calculations that have been made in respect of the Financial Indicators;
- (c) include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;
- (d) be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
- (e) include a history of the Financial Indicators reported by the Supplier in graph form to enable the Authority to easily analyse and assess the trends in financial performance.

3 FINANCIAL DISTRESS EVENTS

3.1 The following shall be Financial Distress Events:

- 3.1.1 an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
- 3.1.2 there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;
- 3.1.3 an FDE Group entity committing a material breach of covenant to its lenders;
- 3.1.4 a Key Sub-contractor notifying the Authority that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;
- 3.1.5 any FDE Group entity extends the filing period for filing its accounts with the Registrar of Companies so that the filing period ends more than 9 months after its accounting reference date without an explanation to the Authority which the Authority (acting reasonably) considers to be adequate;
- 3.1.6 any FDE Group entity is late to file its annual accounts without a public notification or an explanation to the Authority which the Authority, acting reasonably, considers to be adequate;

- 3.1.7 the directors and/or external auditors of any FDE Group entity conclude that a material uncertainty exists in relation to that FDE Group entity's going concern in the annual report including in a reasonable but plausible downside scenario. This includes, but is not limited to, commentary about liquidity and trading prospects in the reports from directors or external auditors;
- 3.1.8 any of the following:
- 3.1.8.1 any FDE Group entity makes a public announcement which contains adverse commentary with regards to that FDE Group entity's liquidity and trading and trading prospects, such as but not limited to, a profit warning or ability to trade as a going concern;
 - 3.1.8.2 commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than [REDACTED] or obligations under a service contract with a total contract value greater than [REDACTED]
 - 3.1.8.3 non-payment by an FDE Group entity of any financial indebtedness;
 - 3.1.8.4 any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
 - 3.1.8.5 the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity;
 - 3.1.8.6 the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;
- in each case which the Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Contract; and
- 3.1.9 any one of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.

4 CONSEQUENCES OF FINANCIAL DISTRESS EVENTS

- 4.1 Immediately upon notification by the Supplier of a Financial Distress Event (or if the Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.5.

Schedule 18 (Financial Distress)

- 4.2 In the event of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1(e), the Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:
- (a) rectify such late or non-payment; or
 - (b) demonstrate to the Authority's reasonable satisfaction that there is a valid reason for late or non-payment.
- 4.3 The Supplier shall (and shall procure that any Monitored Supplier, and/or any relevant Key Sub-contractor shall):
- (a) at the request of the Authority, meet the Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Contract; and
 - (b) where the Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3(a) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Contract:
 - (i) submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing); and
 - (ii) to the extent that it is legally permitted to do so and subject to Paragraph 4.7, provide such information relating to the Supplier, any Monitored Supplier, Key Sub-contractors as the Authority may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.
- 4.4 The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is either:
- (a) approved by the Authority;
 - (b) referred, by notice sent by either Party to the other Party explaining why it thinks the Financial Distress Remediation Plan has not been approved,

to commercial negotiation led by senior representatives who have authority to agree the Financial Distress Remediation Plan to be held within 28 days of the date of the notice; or

(c) finally rejected by the Authority.

4.5 Following approval of the Financial Distress Remediation Plan by the Authority, the Supplier shall:

(a) on a regular basis (which shall not be less than fortnightly):

(i) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Authority, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Services in accordance with this Contract; and

(ii) provide a written report to the Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;

(b) where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.5(a), submit an updated Financial Distress Remediation Plan to the Authority for its approval, and the provisions of Paragraphs 4.4 and 4.5(a) shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and

(c) comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.

4.6 Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.5.

4.7 The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at Paragraph 4.3(b)(ii) is available when required and on request from the Authority and within reasonable timescales. Such measures may include:

(a) obtaining in advance written authority from Key Sub-contractors, and/or Monitored Suppliers authorising the disclosure of the information to the Authority and/or entering into confidentiality agreements which permit disclosure;

(b) agreeing in advance with the Authority, Key Sub-contractors, and/or Monitored Suppliers a form of confidentiality agreement to be entered by

the relevant parties to enable the disclosure of the information to the Authority;

- (c) putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Authority (which may include making price sensitive information available to Authority nominated personnel through confidential arrangements, subject to their consent); and
- (d) disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymisation and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5 FINANCIAL INDICATORS

- 5.1 Subject to the calculation methodology set out at Annex 1 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

Financial Indicator	Calculation ¹	Financial Target Threshold:	Monitoring and Reporting Frequency
1 Operating Margin	<i>[Operating Margin = Operating Profit / Revenue]</i>	>5%	<i>Tested and reported yearly in arrears within 90 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date half year end]</i>
2 Net Debt to EBITDA Ratio	<i>[Net Debt to EBITDA ratio = Net Debt / EBITDA]</i>	<3.5 times	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon EBITDA for the 12 months ending on, and Net Debt at, the relevant accounting reference date</i>
3 Asset Ratio	<i>[Asset Ratio = (Current Assets – Inventories) / Current Liabilities]</i>	> 0.8 times	<i>Tested and reported yearly in arrears within 120 days of each accounting reference date based upon figures at the relevant accounting reference date</i>

Key: ¹ – See Annex 1 of this Schedule which sets out the calculation methodology to be used in the calculation of each Financial Indicator.

6 TERMINATION RIGHTS

- 6.1 The Authority shall be entitled to terminate this Contract under Clause 31.1(b) (*Termination by the Authority*) if:
- (a) the Supplier fails to notify the Authority of a Financial Distress Event in accordance with Paragraph 2.2(b);
 - (b) the Supplier fails to comply with any part of Paragraph 4.3;
 - (c) the Authority finally rejects a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.4 to 4.5(a); and/or
 - (d) the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.5(c).

7 BOARD CONFIRMATION

- 7.1 If this Contract has been specified as a Critical Service Contract under Paragraph 1.1 of Part B to Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*) then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within one hundred and twenty (120) days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Authority in the form set out at Annex 2 of this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:
- (a) that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or
 - (b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.
- 7.2 The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to understand and confirm the position.
- 7.3 In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.
- 7.4 Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Authority (and where the Supplier is a Strategic Supplier, the

Schedule 18 (Financial Distress)

Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

ANNEX 1: CALCULATION METHODOLOGY FOR FINANCIAL INDICATORS

The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

- 1 **Terminology:** The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
- 2 **Groups:** Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
- 3 **Foreign currency conversion:** Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant date for which the Financial Indicator is being calculated.
- 4 **Treatment of non-underlying items:** Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

Financial Indicator	Specific Methodology
1 Operating Margin	<p>The elements used to calculate the Operating Margin should be shown on the face of the Income Statement in a standard set of financial statements.</p> <p>Figures for Operating Profit and Revenue should exclude the entity's share of the results of any joint ventures or Associates.</p> <p>Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero.</p>
2 Net Debt to EBITDA Ratio	<p>"Net Debt" = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</p> <p>"EBITDA" = Operating profit + Depreciation charge + Amortisation charge</p> <p>The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.</p>