**DPS Schedule 6 (Order Form Template and Order Schedules)**

**Order Form**

|  |  |  |
| --- | --- | --- |
| ORDER REFERENCE: |  | CCZP23A07 |
| THE BUYER: |  | Cabinet Office |
| BUYER ADDRESS |  | **REDACTED TEXT under FOIA Section 40, Personal Information.** |
| THE SUPPLIER: |  | Proversity.org Ltd |
| SUPPLIER ADDRESS: |  | **REDACTED TEXT under FOIA Section 40, Personal Information.** |

REGISTRATION NUMBER: **REDACTED TEXT under FOIA Section 40, Personal Information.**

DUNS NUMBER: **REDACTED TEXT under FOIA Section 40, Personal Information.**

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated Friday 6th September 2024

It’s issued under the DPS Contract with the reference number CCZP23A07 for the provision of Support, Maintenance and Development Service.

DPS FILTER CATEGORIES:

TBC AT AWARD

ORDER INCORPORATED TERMS

The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) **RM6219**
3. DPS Special Terms
4. The following Schedules in equal order of precedence:

* Joint Schedules for **RM6219**
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 10 (Rectification Plan)
  + Joint Schedule 11 (Processing Data)
  + Joint Schedule 12 (Supply Chain Visibility)
* Order Schedules for CCZP23A07
  + Order Schedule 1 (Transparency Reports)
  + Order Schedule 2 (Staff Transfer)
  + Order Schedule 3 (Continuous Improvement)
  + [Order Schedule 5 (Pricing Details)
  + [Order Schedule 7 (Key Supplier Staff)
  + [Order  Schedule 8 (Business Continuity and Disaster Recovery)
  + [Order Schedule 9 (Security)
  + [Order Schedule 10 (Exit Management)
  + [Order Schedule 14 (Service Levels)
  + [Order Schedule 15 (Order Contract Management)
  + [Order Schedule 18 (Background Checks)
  + Order Schedule 20 (Order Specification)

1. CCS Core Terms (DPS version) v1.0.3
2. Joint Schedule 5 (Corporate Social Responsibility) RM6219
3. Order Schedule 4 (Order Tender)

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

ORDER SPECIAL TERMS

The following Special Terms are incorporated into this Order Contract:

None

ORDER START DATE: Friday 6th September 2024

ORDER EXPIRY DATE: Friday 5th September 2027

ORDER INITIAL PERIOD: 36 months

DELIVERABLES

See details in Order Schedule 20

MAXIMUM LIABILITY

The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £120,000. Total contract value £300,000.

ORDER CHARGES

See details in Order Schedule 5

REIMBURSABLE EXPENSES

N/A

PAYMENT METHOD

VIA BACS

BUYER’S INVOICE ADDRESS:

Invoices should be submitted to: Shared Services Connected Limited, at email: **REDACTED TEXT under FOIA Section 40, Personal Information.**

BUYER’S AUTHORISED REPRESENTATIVE

**REDACTED TEXT under FOIA Section 40, Personal Information.**

BUYER’S ENVIRONMENTAL POLICY

[https://intranet.cabinetoffice.gov.uk/task/sustainable-development/](https://intranet.cabinetoffice.gov.uk/task/sustainable-development/?_rt=MXwxfGVudmlyb25tZW50YWwgcG9saWN5fDE2NzgxODEwMDY&_rt_nonce=36decd6cd7)

BUYER’S SECURITY POLICY

[https://www.gov.uk/government/publications/security-policy-framework/hmg-securitypolicy-framework](https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

SUPPLIER’S AUTHORISED REPRESENTATIVE

**REDACTED TEXT under FOIA Section 40, Personal Information.**

SUPPLIER’S CONTRACT MANAGER

**REDACTED TEXT under FOIA Section 40, Personal Information.**

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY

Quarterly on the first Working Day of each quarter

KEY STAFF

**REDACTED TEXT under FOIA Section 40, Personal Information.**

**REDACTED TEXT under FOIA Section 40, Personal Information.**

**REDACTED TEXT under FOIA Section 40, Personal Information.**

KEY SUBCONTRACTOR(S)

**REDACTED TEXT under FOIA Section 40, Personal Information.**

E-AUCTIONS

Not applicable

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)]

|  |
| --- |
| **Signed - via Docusign** |
| **Supplier**    <Supplier Sign Here> |
| **REDACTED TEXT under FOIA Section 40, Personal Information.**  Full Name: **REDACTED TEXT under FOIA Section 40, Personal Information.**  Job Title/Role: **REDACTED TEXT under FOIA Section 40, Personal Information.**  Date Signed: 24 Sept 2024 |
| **Buyer**    <Commercial Sign Here> |

DPS Ref: RM6219

Project Version: v1.0

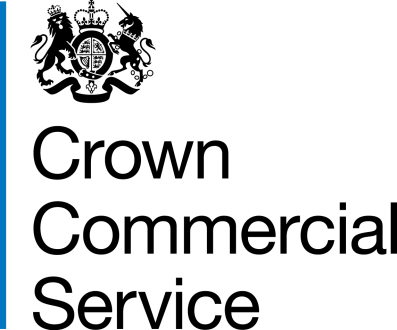
Model Version: v1.3

|  |
| --- |
| Signed: **REDACTED TEXT under FOIA Section 40, Personal Information.**  Full Name: **REDACTED TEXT under FOIA Section 40, Personal Information.**  Job Title/Role: **REDACTED TEXT under FOIA Section 40, Personal Information.**  Date Signed: 25/09/2024 |

DPS Ref: RM6219

Project Version: v1.0

Model Version: v1.3



**Core Terms - DPS**

1. **Definitions used in the contract**

Interpret this Contract using Joint Schedule 1 (Definitions).

1. **How the contract works** 
   1. The Supplier is eligible for the award of Order Contracts during the DPS Contract Period.

* 1. CCS does not guarantee the Supplier any exclusivity, quantity or value of work under the DPS Contract.

* 1. CCS has paid one penny to the Supplier legally to form the DPS Contract. The Supplier acknowledges this payment.

* 1. If the Buyer decides to buy Deliverables under the DPS Contract it must use DPS Schedule 7 (Order Procedure) and must state its requirements using DPS Schedule 6 (Order Form Template and Order Schedules). If allowed by the Regulations, the Buyer can:

* + 1. make changes to DPS Schedule 6 (Order Form Template and Order Schedules);
    2. create new Order Schedules;
    3. exclude optional template Order Schedules; and/or
    4. use Special Terms in the Order Form to add or change terms.

* 1. Each Order Contract:

* + 1. is a separate Contract from the DPS Contract;
    2. is between a Supplier and a Buyer;
    3. includes Core Terms, Schedules and any other changes or items in the completed Order Form; and
    4. survives the termination of the DPS Contract.

* 1. Where the Supplier is approached by any Other Contracting Authority requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this DPS Contract before accepting their order.

* 1. The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

* 1. The Supplier will not be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

* + 1. verify the accuracy of the Due Diligence Information; or (b) properly perform its own adequate checks.

* 1. CCS and the Buyer will not be liable for errors, omissions or misrepresentation of any information.

* 1. The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

* 1. An Order Contract can only be created using the electronic procedures described in the OJEU Notice as required by the Regulations.

* 1. A Supplier can only receive Orders under the DPS Contract while it meets the basic access requirements for the DPS stated in the OJEU Notice. CCS can audit whether a Supplier meets the basic access requirements at any point during the DPS Contract Period.

1. **What needs to be delivered**

## 3.1 All deliverables

**3.1.1** The Supplier must provide Deliverables:

1. that comply with the Specification, the DPS Application and, in relation to an Order Contract, the Order Tender (if there is one);
2. to a professional standard;
3. using reasonable skill and care; (d) using Good Industry Practice;

(e) using its own policies, processes and internal quality control measures as long as they do not conflict with the Contract; (f) on the dates agreed; and (g) that comply with Law.

**3.1.2** The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

## 3.2 Goods clauses

**3.2.1** All Goods delivered must be new, or as new if recycled, unused and of recent origin.

**3.2.2** All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

**3.2.3** The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

**3.2.4** Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

**3.2.5** The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

**3.2.6** The Supplier must deliver the Goods on the date and to the specified location during the Buyer’s working hours.

**3.2.7** The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

**3.2.8** All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

**3.2.9** The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

**3.2.10** The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

**3.2.11** The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier’s reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

**3.2.12** The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer’s option and request) any Goods that the Buyer rejects because they do not conform with Clause 3. If the Supplier does not do this it will pay the Buyer’s costs including repair or re-supply by a third party.

## 3.3 Services clauses

**3.3.1** Late Delivery of the Services will be a Default of an Order Contract.

**3.3.2** The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

**3.3.3** The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

**3.3.4** The Supplier must allocate sufficient resources and appropriate expertise to each Contract.

**3.3.5** The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer’s operations, employees or other contractors.

**3.3.6** The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

**3.3.7** The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

1. **Pricing and payments** 
   1. In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.

* 1. CCS must invoice the Supplier for the Management Levy and the Supplier must pay it using the process in DPS Schedule 5 (Management Levy and Information).

* 1. All Charges and the Management Levy:

* + 1. exclude VAT, which is payable on provision of a valid VAT invoice; and (b) include all costs connected with the Supply of Deliverables.

* 1. The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

* 1. A Supplier invoice is only valid if it:

* + 1. includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer;
    2. includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any); and
    3. does not include any Management Levy (the Supplier must not charge the Buyer in any way for the Management Levy).

* 1. The Buyer must accept and process for payment an undisputed Electronic Invoice received from the Supplier.

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

* 1. The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, CCS or the Buyer can publish the details of the late payment or non-payment.

* 1. If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables, then CCS or the Buyer may require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items.

* 1. If CCS or the Buyer uses Clause 4.9 then the DPS Pricing (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

* 1. The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.

1. **The buyer’s obligations to the supplier** 
   1. If Supplier Non-Performance arises from an Authority Cause:

* + 1. neither CCS or the Buyer can terminate a Contract under Clause 10.4.1;
    2. the Supplier is entitled to reasonable and proven additional expenses and to relief from liability and Deduction under this Contract;
    3. the Supplier is entitled to additional time needed to make the Delivery; and
    4. the Supplier cannot suspend the ongoing supply of Deliverables.

* 1. Clause 5.1 only applies if the Supplier:

* + 1. gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware;
    2. demonstrates that the Supplier Non-Performance would not have occurred but for the Authority Cause; and
    3. mitigated the impact of the Authority Cause.

1. **Record keeping and reporting** 
   1. The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

* 1. The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract:

* + 1. during the Contract Period;
    2. for 7 years after the End Date; and (c) in accordance with UK GDPR, including but not limited to the records and accounts stated in the definition of Audit in Joint Schedule 1.

* 1. The Relevant Authority or an Auditor can Audit the Supplier.

* 1. During an Audit, the Supplier must:

* + 1. allow the Relevant Authority or any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit; and
    2. provide information to the Relevant Authority or to the Auditor and reasonable co-operation at their request.

* 1. Where the Audit of the Supplier is carried out by an Auditor, the Auditor shall be entitled to share any information obtained during the Audit with the Relevant Authority.

* 1. If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

* + 1. tell the Relevant Authority and give reasons;
    2. propose corrective action; and
    3. provide a deadline for completing the corrective action.

* 1. The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

* + 1. the methodology of the review;
    2. the sampling techniques applied; (c) details of any issues; and (d) any remedial action taken.

* 1. The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier’s management team that is qualified in either a relevant audit or financial discipline.

1. **Supplier staff** 
   1. The Supplier Staff involved in the performance of each Contract must:

* + 1. be appropriately trained and qualified;
    2. be vetted using Good Industry Practice and the Security Policy; and (c) comply with all conduct requirements when on the Buyer’s Premises.

* 1. Where a Buyer decides one of the Supplier’s Staff is not suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

* 1. If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

* 1. The Supplier must provide a list of Supplier Staff needing to access the Buyer’s Premises and say why access is required.

* 1. The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

1. **Rights and protection** 
   1. The Supplier warrants and represents that:

* + 1. it has full capacity and authority to enter into and to perform each Contract;
    2. each Contract is executed by its authorised representative;
    3. it is a legally valid and existing organisation incorporated in the place it was formed;
    4. there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract;
    5. it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract;
    6. it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract;
    7. it is not impacted by an Insolvency Event; and (h) it will comply with each Order Contract.

* 1. The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

* 1. The Supplier indemnifies both CCS and every Buyer against each of the following:

* + 1. wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract; and (b) non-payment by the Supplier of any Tax or National Insurance.

* 1. All claims indemnified under this Contract must use Clause 26.

* 1. The description of any provision of this Contract as a warranty does not prevent CCS or a Buyer from exercising any termination right that it may have for breach of that clause by the Supplier.

* 1. If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

* 1. All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer’s benefit by the Supplier.

1. **Intellectual Property Rights (IPRs)** 
   1. Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier’s Existing IPR to enable it to both:

* + 1. receive and use the Deliverables; and
    2. make use of the deliverables provided by a Replacement Supplier.

* 1. Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.

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

* 1. Neither Party has the right to use the other Party’s IPRs, including any use of the other Party’s names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

* 1. If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

* 1. If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer’s sole option, either:

* + 1. obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR; or
    2. replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.

* 1. In spite of any other provisions of a Contract and for the avoidance of doubt, award of a Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific IPR involved.

1. **Ending the contract or any subcontract**

## 10.1 Contract Period

**10.1.1** The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

**10.1.2** The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

## 10.2 Ending the contract without a reason

**10.2.1** CCS has the right to terminate the DPS Contract at any time without reason by giving the Supplier at least 30 days' notice.

**10.2.2** Each Buyer has the right to terminate their Order Contract at any time without reason by giving the Supplier not less than 90 days' written notice.

## 10.3 Rectification plan process

**10.3.1** If there is a Default, the Relevant Authority may, without limiting its other rights, request that the Supplier provide a Rectification Plan.

**10.3.2** When the Relevant Authority receives a requested Rectification Plan it can either:

1. reject the Rectification Plan or revised Rectification Plan, giving reasons; or
2. accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties.

**10.3.3** Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

1. must give reasonable grounds for its decision; and
2. may request that the Supplier provides a revised Rectification Plan within 5 Working Days.

**10.3.4**  If the Relevant Authority rejects any Rectification Plan, including any revised Rectification Plan, the Relevant Authority does not have to request a revised Rectification Plan before exercising its right to terminate its Contract under Clause 10.4.3(a).

## 10.4 When CCS or the buyer can end a contract

**10.4.1** If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

1. there is a Supplier Insolvency Event;
2. there is a Default that is not corrected in line with an accepted Rectification Plan;
3. the Supplier does not provide a Rectification Plan within 10 days of the request;
4. there is any material Default of the Contract;
5. there is any material Default of any Joint Controller Agreement relating to any Contract;
6. there is a Default of Clauses 2.10, 9, 14, 15, 27, 32 or DPS Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract;
7. there is a consistent repeated failure to meet the Performance Indicators in DPS Schedule 4 (DPS Management);
8. there is a Change of Control of the Supplier which is not pre-approved by the Relevant Authority in writing;
9. if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded; or
10. the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them.

**10.4.2** CCS may terminate the DPS Contract if a Buyer terminates an Order Contract for any of the reasons listed in Clause 10.4.1.

**10.4.3** If any of the following non-fault based events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

1. the Relevant Authority rejects a Rectification Plan;
2. there is a Variation which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes);
3. if there is a declaration of ineffectiveness in respect of any Variation; or (d) any of the events in 73 (1) (a) or (c) of the Regulations happen.

## 10.5 When the supplier can end the contract

The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate an Order Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

## 10.6 What happens if the contract ends

**10.6.1** Where a Party terminates a Contract under any of Clauses 10.2.1, 10.2.2, 10.4.1, 10.4.2, 10.4.3, 10.5 or

20.2 or a Contract expires all of the following apply:

1. The Buyer’s payment obligations under the terminated Contract stop immediately.
2. Accumulated rights of the Parties are not affected.
3. The Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the End Date.
4. The Supplier must promptly delete or return the Government Data except where required to retain copies by Law.
5. The Supplier must promptly return any of CCS or the Buyer’s property provided under the terminated Contract.
6. The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and reprocurement (including to a Replacement Supplier).

**10.6.2** In addition to the consequences of termination listed in Clause 10.6.1, where the Relevant Authority terminates a Contract under Clause 10.4.1 the Supplier is also responsible for the Relevant Authority’s reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

**10.6.3** In addition to the consequences of termination listed in Clause 10.6.1, if either the Relevant Authority terminates a Contract under Clause 10.2.1 or 10.2.2 or a Supplier terminates an Order Contract under Clause 10.5:

1. the Buyer must promptly pay all outstanding Charges incurred to the Supplier; and
2. the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated.

**10.6.4** In addition to the consequences of termination listed in Clause 10.6.1, where a Party terminates under Clause 20.2 each Party must cover its own Losses.

**10.6.5** The following Clauses survive the termination or expiry of each Contract: 3.2.10, 4.2, 6, 7.5, 9, 11, 12.2, 14, 15, 16, 17, 18, 31.3, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

## 10.7 Partially ending and suspending the contract

**10.7.1** Where CCS has the right to terminate the DPS Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Order Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Order Contracts that have already been signed.

**10.7.2** Where CCS has the right to terminate a DPS Contract it is entitled to terminate all or part of it.

**10.7.3** Where the Buyer has the right to terminate an Order Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

**10.7.4**  The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

**10.7.5** The Parties must agree any necessary Variation required by Clause 10.7 using the Variation Procedure, but the Supplier may not either:

1. reject the Variation; or
2. increase the Charges, except where the right to partial termination is under Clause 10.2.

**10.7.6** The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.7.

## 10.8 When subcontracts can be ended

At the Buyer’s request, the Supplier must terminate any Subcontracts in any of the following events:

1. there is a Change of Control of a Subcontractor which is not pre-approved by the Relevant Authority in writing;
2. the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4; or
3. a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority.

1. **How much you can be held responsible for** 
   1. Each Party's total aggregate liability in each Contract Year under this DPS Contract (whether in tort, contract or otherwise) is no more than £1,000,000.

* 1. Each Party's total aggregate liability in each Contract Year under each Order Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Order Form.

* 1. No Party is liable to the other for:

* + 1. any indirect Losses; or
    2. Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

* 1. In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

* + 1. its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
    2. its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;
    3. any liability that cannot be excluded or limited by Law;
    4. its obligation to pay the required Management Levy or Default Management Levy.

* 1. In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3(b), 9.5, 31.3 or Order Schedule 2 (Staff Transfer) of a Contract.

* 1. In spite of Clauses 11.1, 11.2 but subject to Clauses 11.3 and 11.4, the Supplier's aggregate liability in each and any Contract Year under each Contract under Clause 14.8 shall in no event exceed the Data Protection Liability Cap.

* 1. Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

* 1. When calculating the Supplier’s liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

* + 1. Deductions; and
    2. any items specified in Clauses 11.5 or 11.6.

* 1. If more than one Supplier is party to a Contract, each Supplier Party is jointly and severally liable for their obligations under that Contract.

1. **Obeying the law** 
   1. The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

* 1. To the extent that it arises as a result of a Default by the Supplier, the Supplier indemnifies the Relevant Authority against any fine or penalty incurred by the Relevant Authority pursuant to Law and any costs incurred by the Relevant Authority in defending any proceedings which result in such fine or penalty.

* 1. The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

1. **Insurance**

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

1. **Data protection** 
   1. The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

* 1. The Supplier must not remove any ownership or security notices in or relating to the Government Data.

* 1. The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

* 1. The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

* 1. If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

* 1. If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

* + 1. tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
    2. restore the Government Data itself or using a third party.

* 1. The Supplier must pay each Party’s reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.

* 1. The Supplier:

* + 1. must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request;
    2. must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
    3. must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
    4. securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it; and
    5. indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

1. **What you must keep confidential** 
   1. Each Party must:

* + 1. keep all Confidential Information it receives confidential and secure;
    2. except as expressly set out in the Contract at Clauses 15.2 to 15.4 or elsewhere in the Contract, not disclose, use or exploit the Disclosing Party’s Confidential Information without the Disclosing Party's prior written consent; and
    3. immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

* 1. In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

* + 1. where disclosure is required by applicable Law or by a court with the relevant jurisdiction if, to the extent not prohibited by Law, the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
    2. if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party;
    3. if the information was given to it by a third party without obligation of confidentiality;
    4. if the information was in the public domain at the time of the disclosure;
    5. if the information was independently developed without access to the Disclosing Party’s Confidential Information;
    6. on a confidential basis, to its auditors;
    7. on a confidential basis, to its professional advisers on a need-to-know basis; or
    8. to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

* 1. In spite of Clause 15.1, the Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

* 1. In spite of Clause 15.1, CCS or the Buyer may disclose Confidential Information in any of the following cases:

* + 1. on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer;
    2. on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to;
    3. if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
    4. where requested by Parliament; or (e) under Clauses 4.7 and 16.

* 1. For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

* 1. Transparency Information is not Confidential Information.

* 1. The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

1. **When you can share information** 
   1. The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

* 1. Within five (5) Working Days of the Buyer’s request the Supplier must give CCS and each Buyer full cooperation and information needed so the Buyer can:

* + 1. publish the Transparency Information;
    2. comply with any Freedom of Information Act (FOIA) request; and/or
    3. comply with any Environmental Information Regulations (EIR) request.

* 1. The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority’s decision in its absolute discretion.

1. **Invalid parts of the contract**

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it is valid or enforceable.

1. **No other terms apply**

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements, agreements and any course of dealings made between the Parties, whether written or oral, in relation to its subject matter. No other provisions apply.

1. **Other people’s rights in a contract**

No third parties may use the Contracts (Rights of Third Parties) Act 1999 (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

1. **Circumstances beyond your control** 
   1. Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

* + 1. provides a Force Majeure Notice to the other Party; and
    2. uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

* 1. Either Party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

1. **Relationships created by the contract**

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

1. **Giving up contract rights**

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

1. **Transferring responsibilities** 
   1. The Supplier cannot assign, novate or transfer a Contract or any part of a Contract without the Relevant Authority’s written consent.

* 1. The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Central

Government Body, public or private sector body which performs the functions of the Relevant Authority.

* 1. When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

* 1. The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

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

* 1. If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

* + 1. their name;
    2. the scope of their appointment; and (c) the duration of their appointment.

1. **Changing the contract** 
   1. Either Party can request a Variation which is only effective if agreed in writing and signed by both Parties.

* 1. The Supplier must provide an Impact Assessment either:

* + 1. with the Variation Form, where the Supplier requests the Variation; or
    2. within the time limits included in a Variation Form requested by CCS or the Buyer.

* 1. If the Variation cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

* + 1. agree that the Contract continues without the Variation; or
    2. terminate the affected Contract, unless in the case of an Order Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them; or
    3. refer the Dispute to be resolved using Clause 34 (Resolving Disputes).

* 1. CCS and the Buyer are not required to accept a Variation request made by the Supplier.

* 1. If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the DPS Pricing or the Charges.

* 1. If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, DPS Pricing or a Contract and provide evidence:

* + 1. that the Supplier has kept costs as low as possible, including in Subcontractor costs; and (b) of how it has affected the Supplier’s costs.

* 1. Any change in the DPS Pricing or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

* 1. For 101(5) of the Regulations, if the Court declares any Variation ineffective, the Parties agree that their mutual rights and obligations will be regulated by the terms of the Contract as they existed immediately prior to that Variation and as if the Parties had never entered into that Variation.

1. **How to communicate about the contract** 
   1. All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they are delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9:00am on the first Working Day after sending unless an error message is received.

* 1. Notices to CCS must be sent to the CCS Authorised Representative’s address or email address indicated on the Platform.

* 1. Notices to the Buyer must be sent to the Buyer Authorised Representative’s address or email address in the Order Form.

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

1. **Dealing with claims** 
   1. If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

* 1. At the Indemnifier’s cost the Beneficiary must both:

* + 1. allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and (b) give the Indemnifier reasonable assistance with the claim if requested.

* 1. The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.

* 1. The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary’s reputation.

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

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

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

* + 1. the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or
    2. the amount the Indemnifier paid the Beneficiary for the Claim.

1. **Preventing fraud, bribery and corruption** 
   1. The Supplier must not during any Contract Period:

* + 1. commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2); or
    2. do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

* 1. The Supplier must during the Contract Period:

* + 1. create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same;
    2. keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request; and
    3. if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

* 1. The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses

27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

* + 1. been investigated or prosecuted for an alleged Prohibited Act;
    2. been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency;
    3. received a request or demand for any undue financial or other advantage of any kind related to a Contract; or
    4. suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act.

* 1. If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

* 1. In any notice the Supplier gives under Clause 27.3 it must specify the:

* + 1. Prohibited Act;
    2. identity of the Party who it thinks has committed the Prohibited Act; and (c) action it has decided to take.

1. **Equality, diversity and human rights** 
   1. The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

* + 1. protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
    2. any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law.

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

1. **Health and safety** 
   1. The Supplier must perform its obligations meeting the requirements of:

* + 1. all applicable Law regarding health and safety; and
    2. the Buyer’s current health and safety policy while at the Buyer’s Premises, as provided to the Supplier.

* 1. The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they are aware of at the Buyer Premises that relate to the performance of a Contract.

1. **Environment** 
   1. When working on Site the Supplier must perform its obligations under the Buyer’s current Environmental Policy, which the Buyer must provide.

* 1. The Supplier must ensure that Supplier Staff are aware of the Buyer’s Environmental Policy.

1. **Tax** 
   1. The Supplier must not breach any Tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor Tax or social security contribution.

* 1. Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

* + 1. the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant; and
    2. other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need.

* 1. Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under an Order Contract, the Supplier must both:

* + 1. comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
    2. indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

* 1. If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

* + 1. the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
    2. the Worker’s contract may be terminated at the Buyer’s request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
    3. the Worker’s contract may be terminated at the Buyer’s request if the Worker provides information which the Buyer considers is not good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements; and
    4. the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

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

* 1. The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

* 1. CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

1. **Reporting a breach of the contract** 
   1. As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

* + 1. Law;
    2. Clause 12.1; or (c) Clauses 27 to 32.

* 1. The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

1. **Resolving disputes** 
   1. If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

* 1. If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the

Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the

Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

* 1. Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

* + 1. determine the Dispute;
    2. grant interim remedies; and/or
    3. grant any other provisional or protective relief.

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

* 1. The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must

do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

* 1. The Supplier cannot suspend the performance of a Contract during any Dispute.

1. **Which law applies**

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

**Order Schedule 1 (Transparency Reports)**

Order Ref:

Crown Copyright 2021

**Order Schedule 1 (Transparency Reports)**

* 1. The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1

[(https://www.gov.uk/government/publications/procurement-policy-note-0117update-to-transparency-principles)](https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

* 1. Without prejudice to the Supplier's reporting requirements set out in the DPS

Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

* 1. If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

* 1. The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

DPS Ref: RM6219 Learning and Training

Project Version: v1.0 1

Model Version: v1.0

**Order Schedule 1 (Transparency Reports)**

Order Ref:

Crown Copyright 2021

**Annex A: List of Transparency Reports**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Content** | **Format** | **Frequency** |
| Purchase Order Status | Purchase  Order and  Invoice  Report | Report | Monthly |
| Key Subcontractors | Subcontract ors in use and  activities being worked on. Security  Clearance  Level | Report | Quarterly |
| Pricing and Cost  Breakdown Information | Total Charges for current month with breakdown. Total charges expected for the next month with breakdown. | Report | Monthly |

DPS Ref: RM6219 Learning and Training

Project Version: v1.0 2 Model Version: v1.0 **Order Schedule 3 (Continuous Improvement)** Order Ref:

Crown Copyright2021

**Order Schedule 3 (Continuous Improvement)**

## 1. Buyer’s Rights

1.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

## 2. Supplier’s Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer’s costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

2.3.1 identifying the emergence of relevant new and evolving technologies;

2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

2.3.4 measuring and reducing the sustainability impacts of the

Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred

DPS Ref: RM6219 Learning and Training

1

**Order Schedule 3 (Continuous Improvement)** Order Ref:

Crown Copyright2021

(100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed

Continuous Improvement Plan or any updates to it within twenty (20) Working

Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working

Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

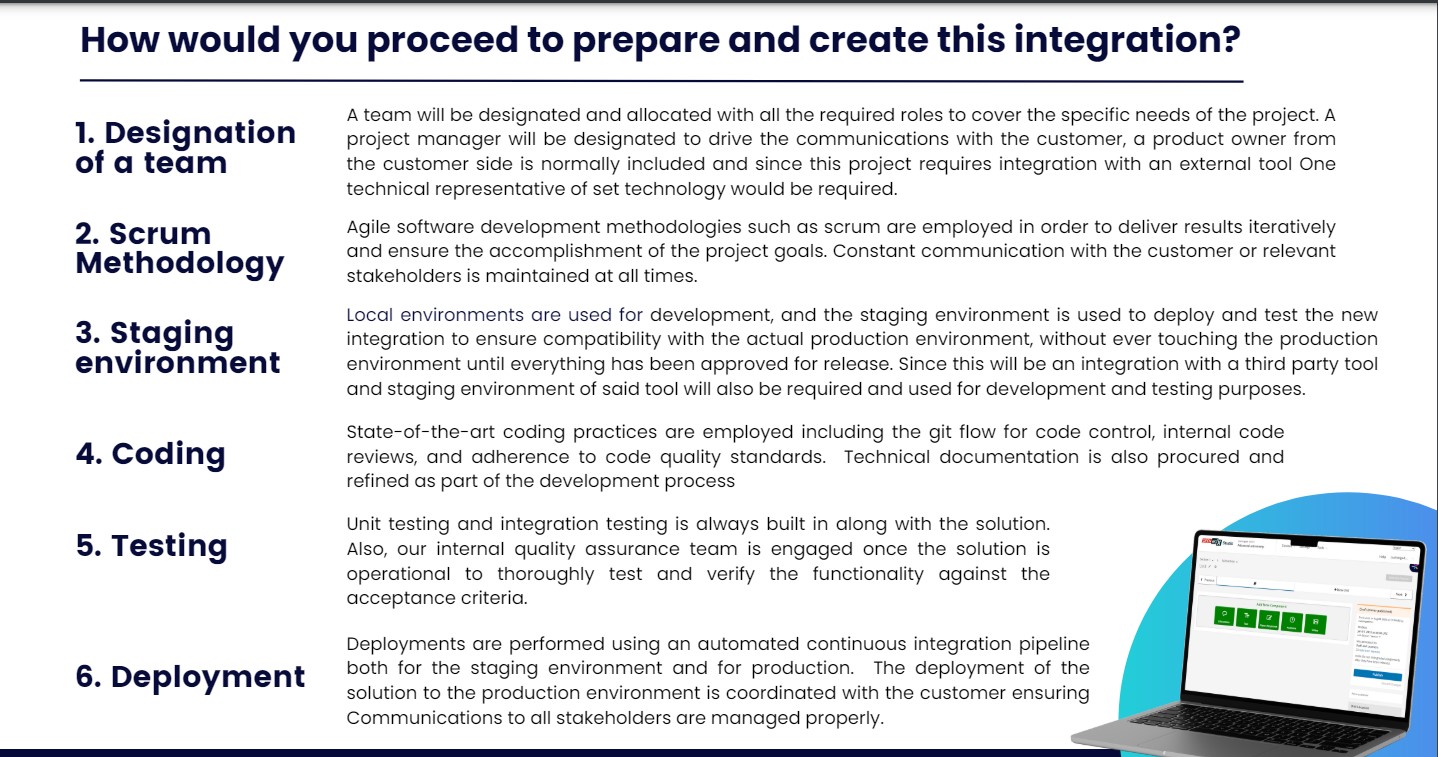
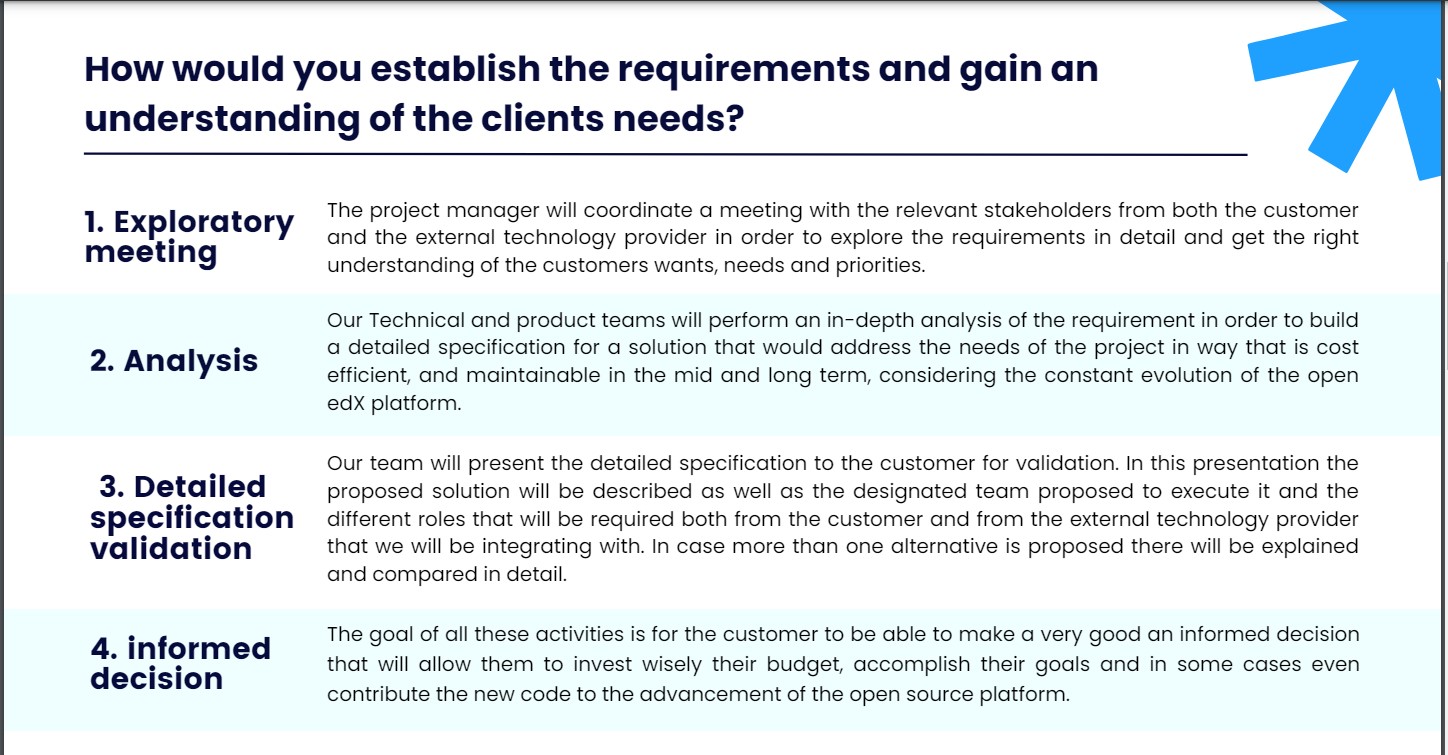
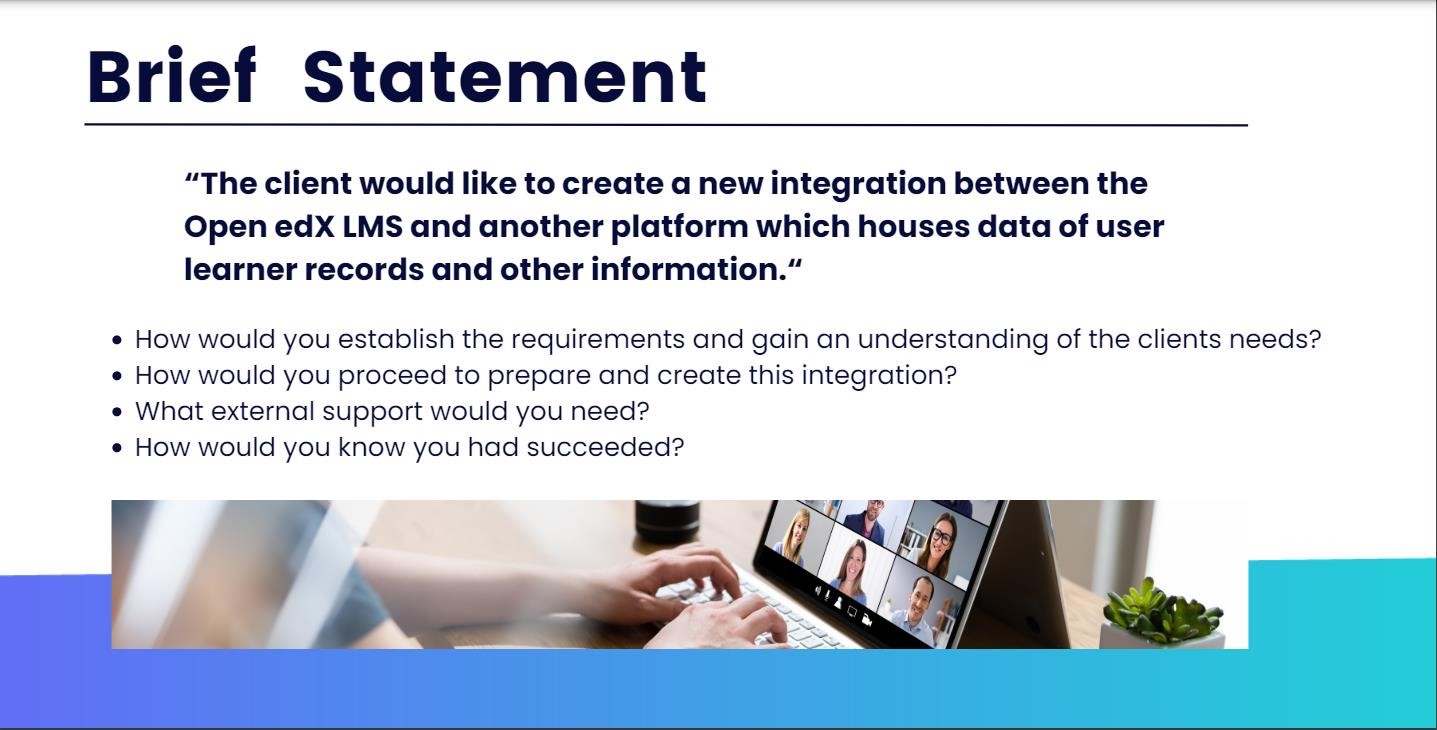
2.12 At any time during the Contract Period of the Order Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

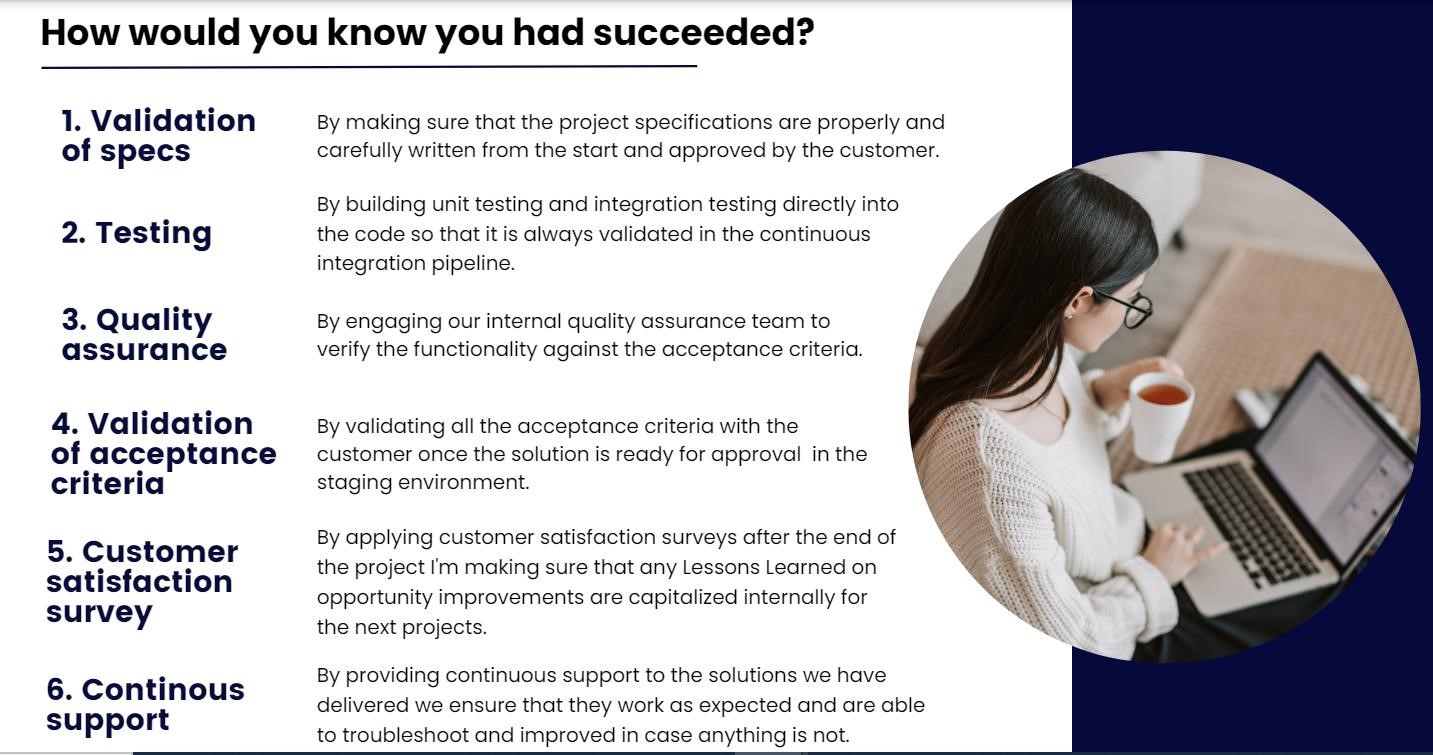
DPS Ref: RM6219 Learning and Training

2

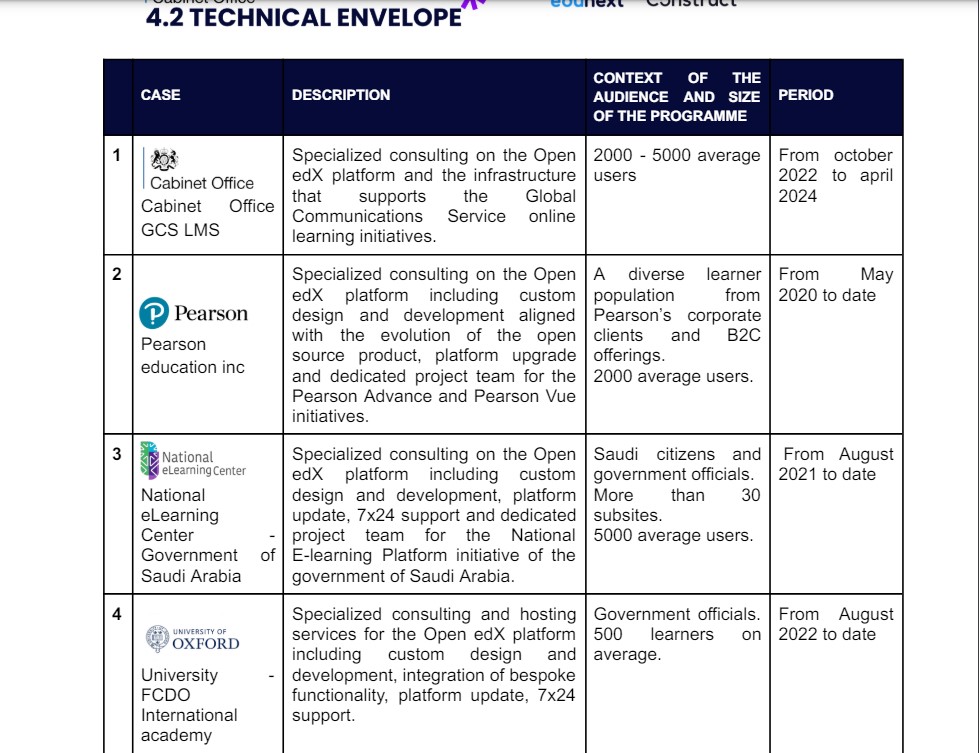
**Order Schedule 4 (Order Tender)**

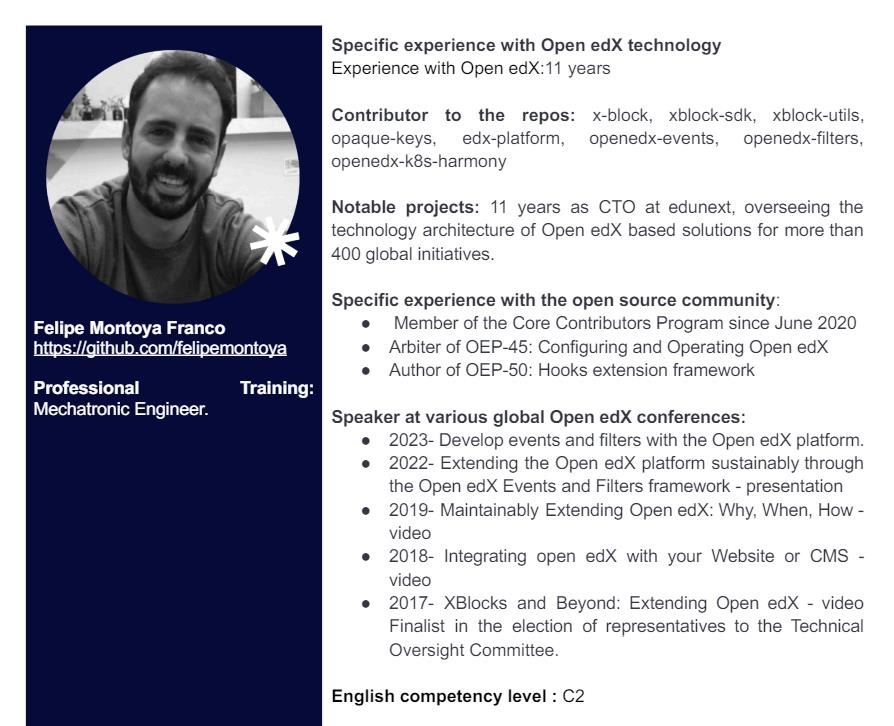
## 4.1





4.2



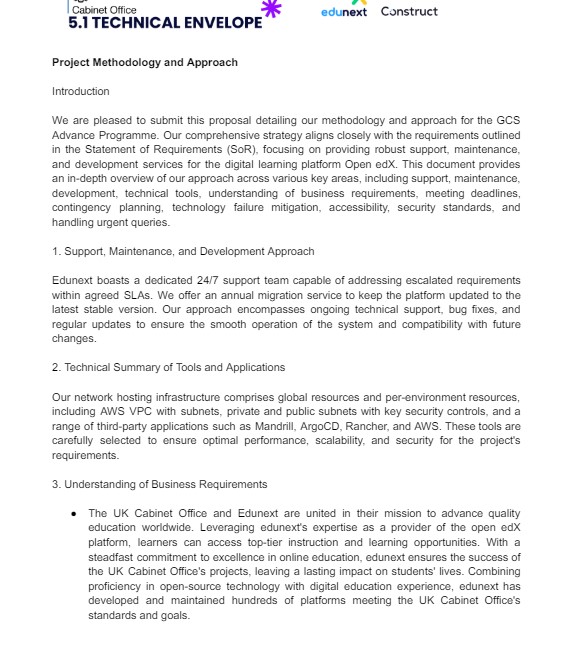


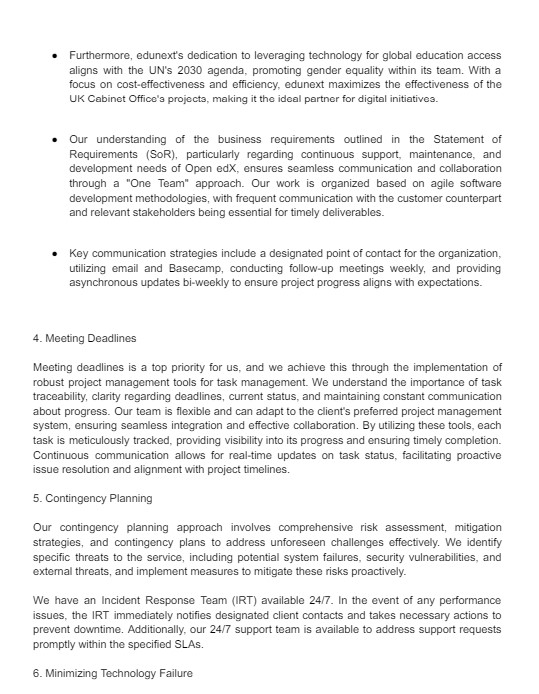


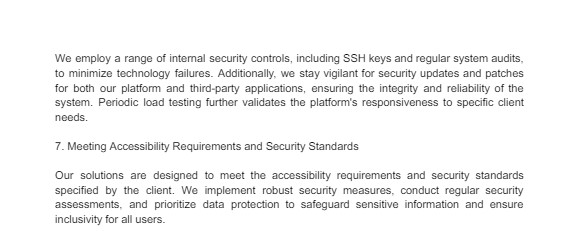




5.1

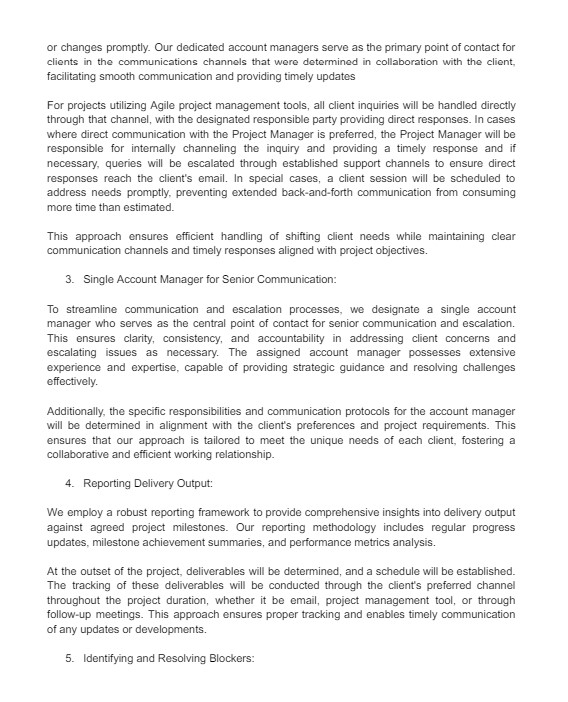


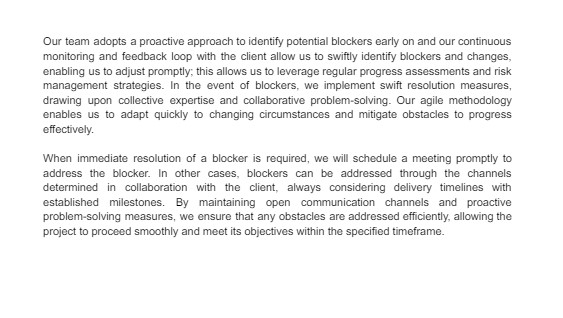




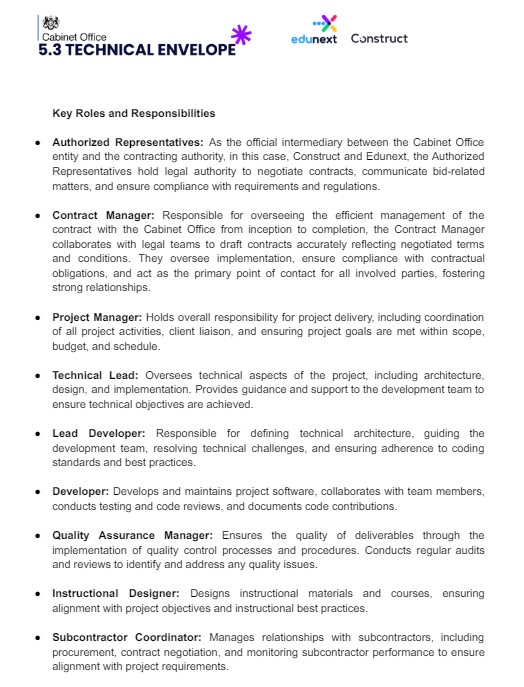
5.2







5.3

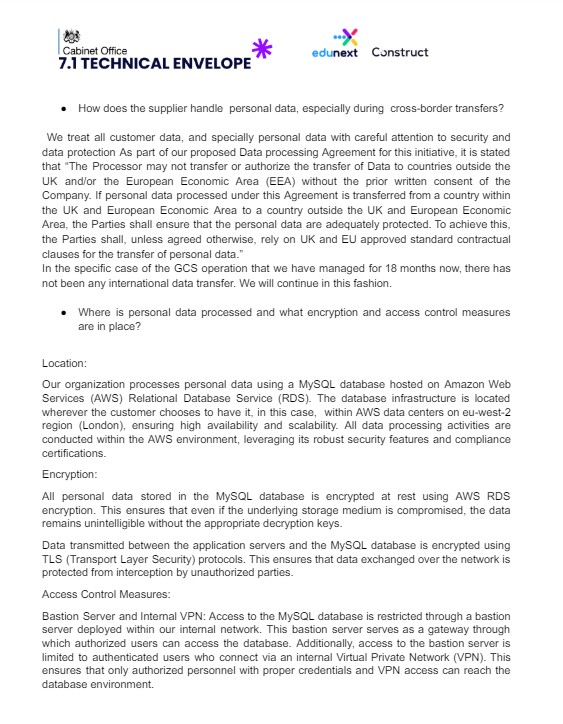


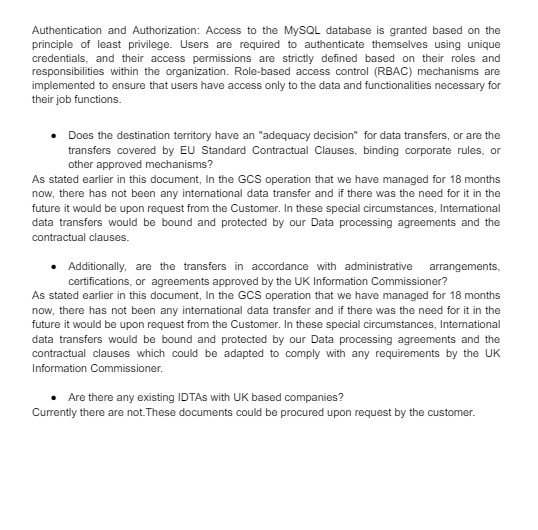


5.4

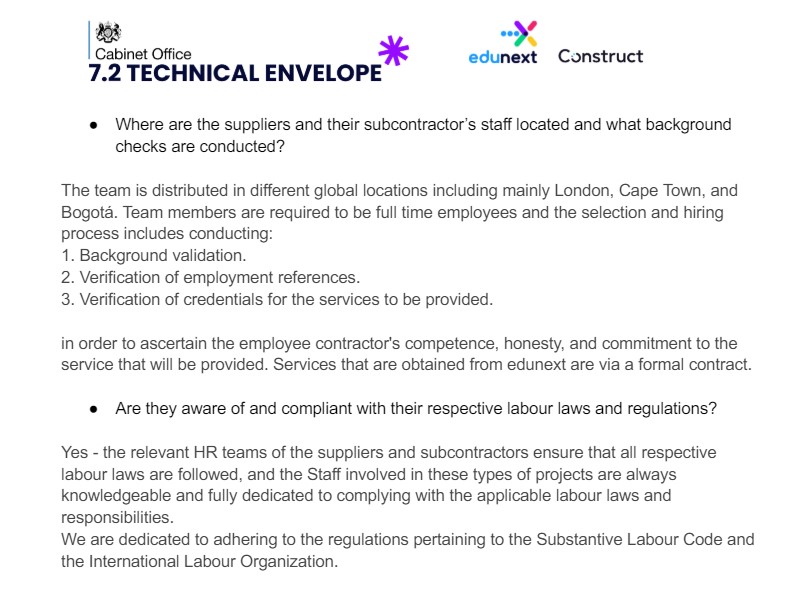


7.1

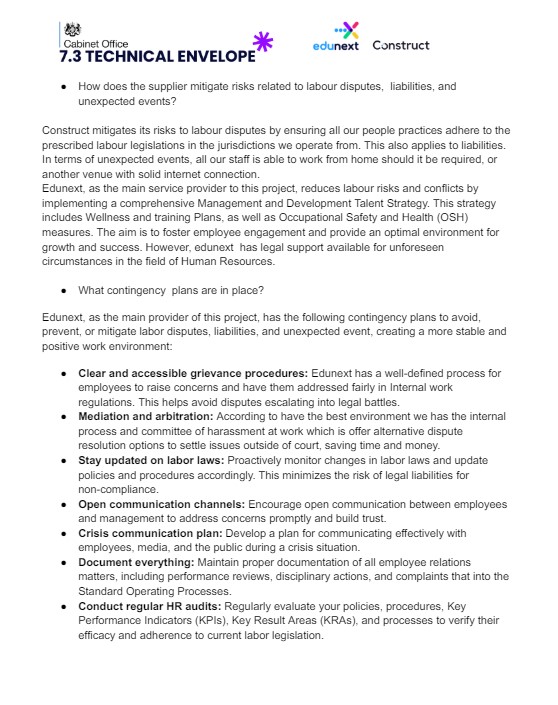




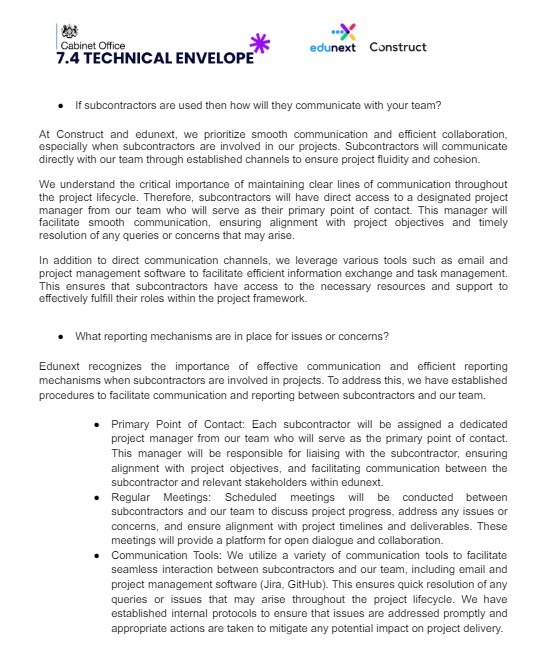
7.2



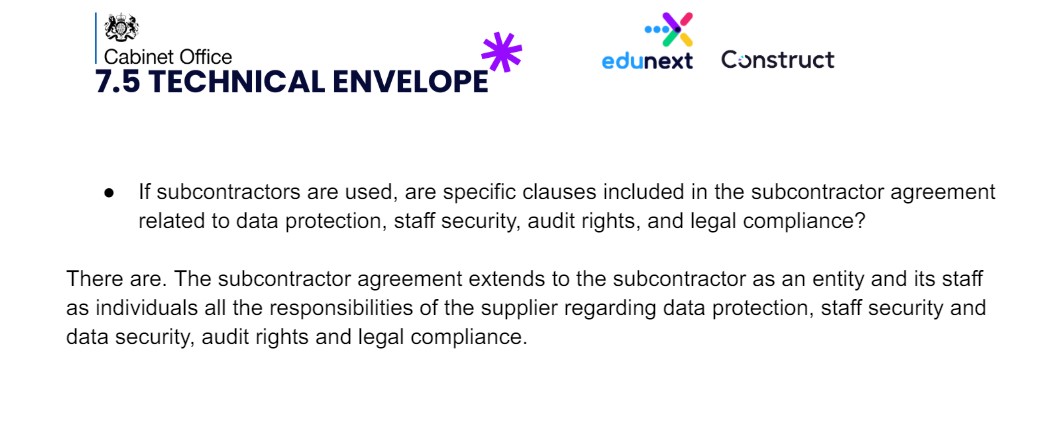
7.3



7.4



7.5



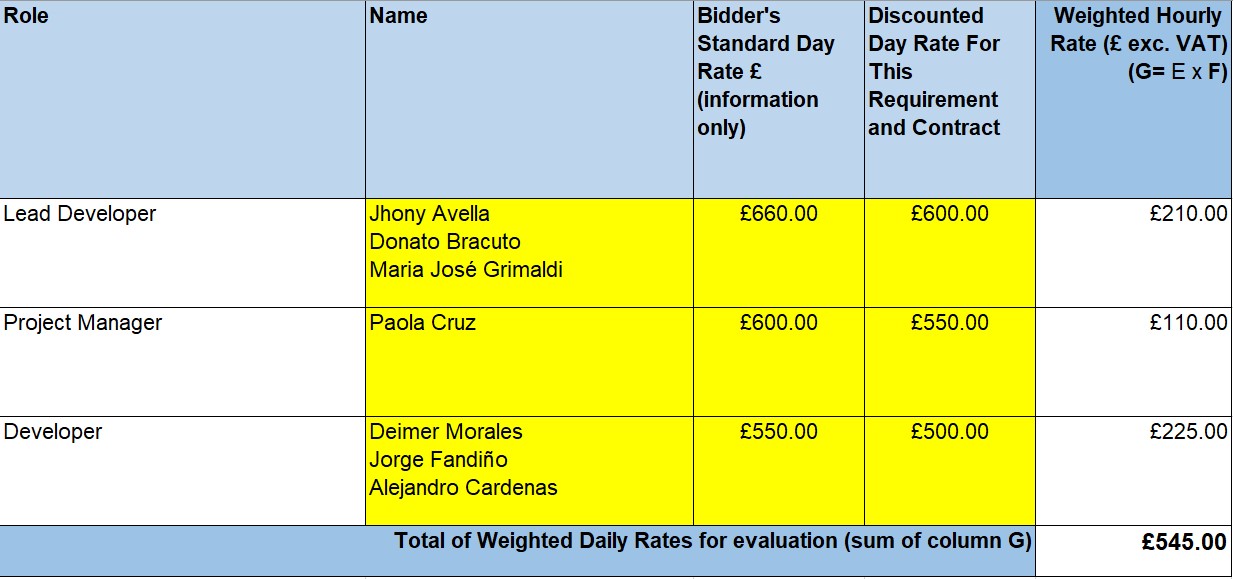
**Order Schedule 5 (Pricing Details)** Order Ref:

Crown Copyright 2021

**Order Schedule 5 (Pricing Details)**

As provided by the supplier as their commercial submission:

**Core Rates:**



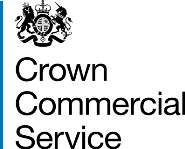
## Scenario Costs

The Total Contract Value of £360,000.00 excluding VAT is inclusive of the optional extension option

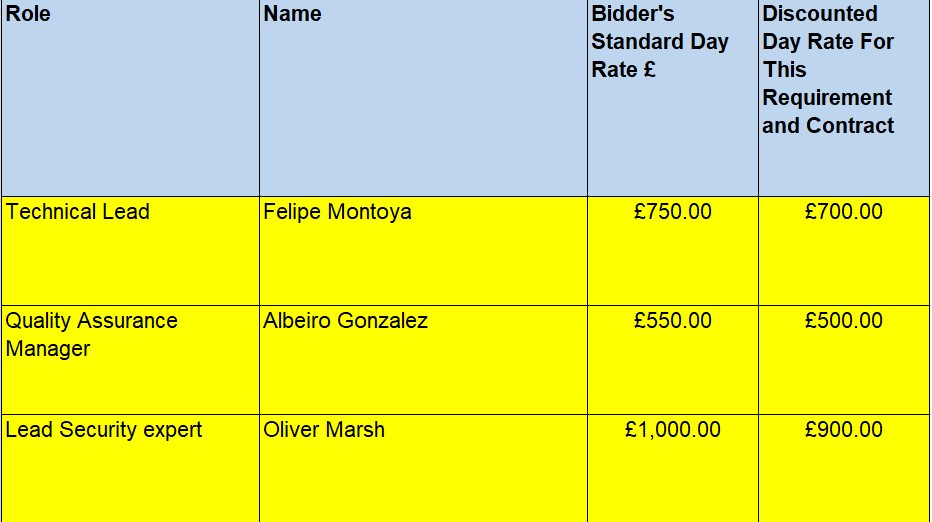


## Other Roles Cost (Info Only)

1

**Call-Off Schedule 5 (Call-Off Pricing)**

Crown Copyright 2017



Ref: RM3830

FM Project Version: 1.A

**Order Schedule 7 (Key Supplier Staff)**

1.1 The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or longterm sick leave; or

1.4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least three (3) Months’ notice;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

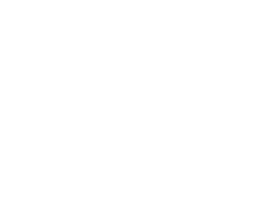
1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

**Annex 1- Key Roles**

|  |  |  |
| --- | --- | --- |
| **Key Role** | **Key Staff** | **Contract Details** |
| Account Director | John Jeppsson | john@constructeducation. com |
| Data Protection Officer | Ian Mafuta | ian@constructeducation.c om |
| CEO | Lorcan McHugh | lorcan@constructeducatio  n.com |
|  |  |  |
|  |  |  |
|  |  |  |

Schedule [\*\*\*\*\*] (Security

Management: (Developer)



|

## 1 Buyer Options

Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

|  |  |  |
| --- | --- | --- |
| **Buyer risk assessment** (see Paragraph 2) | |  |
| The Buyer has assessed this Agreement as: | a higher-risk agreement | ☐ |
| a standard agreement | ☒ |
| **Certifications** (see Paragraph 8) (applicable only for standard risk agreements) | |  |
| Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must have the following Certifications: | Cyber Essentials Plus | ☒ |
| Cyber Essentials | ☐ |
| **Locations** (see Paragraph 1 of the Security Requirements) | |  |
| The Supplier and Sub-contractors may store, access or Process Government Data in: | the United Kingdom only | ☐ |
| the United Kingdom and European Economic Area only | ☐ |
| anywhere in the world not prohibited by the Buyer | ☒ |
| **Support Locations** (see Paragraph 1 of the Security Requirements) | |  |
| The Supplier and Subcontractors may operate Support Locations in: | the United Kingdom only | ☐ |
| the United Kingdom and European Economic Area only | ☐ |
| anywhere in the world not prohibited by the Buyer | ☒ |

## 2 Buyer risk assessment

2.1 Where the Buyer has assessed this Agreement as a higher-risk agreement, the Supplier must:

1. comply with all requirements of this Schedule [♦] (*Security Management*); and
2. hold the ISO/IEC 27001:2013 Relevant Certification from a UKAS-approved certification body (see Paragraph 8).

2.2 Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must comply with all requirements of this this Schedule [♦] (*Security Management*) except:

1. Paragraph 9 (*Security Management Plan*);
2. paragraph 9 of the Security Requirements (*Code Reviews*);
3. paragraph 11 of the Security Requirements (*Third-party Software Modules*);
4. paragraph 12 of the Security Requirements (*Hardware and software support*);
5. paragraph 13 of the Security Requirements (*Encryption*); and
6. paragraph 19 of the Security Requirements (*Access Control*).

2.3 Where the Buyer has not made an assessment in the table in Paragraph 1, the Parties must treat this Agreement as a higher-risk agreement.

## 3 Definitions

3.1 In this Schedule [♦] (*Security Management*):

|  |  |
| --- | --- |
| **“Anti-virus**  **Software”** | means software that:   1. protects the Supplier Information Management System from the possible introduction of Malicious Software; 2. scans for and identifies possible Malicious Software in the Supplier Information Management System; 3. if Malicious Software is detected in the Supplier Information Management System, so far as possible:    1. prevents the harmful effects of the   Malicious Software; and   * 1. removes the Malicious Software from the Supplier Information Management System; |
| **“Breach Action**  **Plan”** | means a plan prepared under paragraph 22.3 of the Security Requirements addressing any Breach of Security; |
| **“Breach of**  **Security”** | means the occurrence of: |

|  |  |  |
| --- | --- | --- |
|  | **(a)** | any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code; |
|  | **(d)** | the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code; and/or |
|  | **(e)** | any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; |
|  | **(f)** | the installation of Malicious Software in the:   1. Supplier Information Management   System;   1. Development Environment; or 2. Developed System; |
|  | **(g)** | any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:   1. Supplier Information Management   System;   1. Development Environment; or 2. Developed System; and |
|  | **(h)** | includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:   1. was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or 2. was undertaken, or directed by, a state other than the United Kingdom |
| **“Buyer Data”** | means any:  **(a)** | 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; |
|  | **(b)** | Personal Data for which the Buyer is a, or the, Data Controller; or |
|  | **(c)** | any meta-data relating to categories of data referred to in paragraphs (a) or (b); |
|  | that is:  **(a)** | supplied to the Supplier by or on behalf of the Buyer; or |

|  |  |
| --- | --- |
|  | **(b)** that the Supplier generates, processes, stores or transmits under this Agreement; and  for the avoidance of doubt includes the Code and any meta-data relating to the Code. |
| **“Buyer Data**  **Register”** | means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 23 of the Security Requirements; |
| **“Buyer**  **Equipment”** | means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System; |
| **“Buyer System”** | means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services; |
| **“Certification**  **Default”** | means the occurrence of one or more of the circumstances listed in Paragraph 8.4; |
| **“Certification**  **Rectification Plan”** | means the plan referred to in Paragraph 8.5(a); |
| **“Certification Requirements”** | means the requirements set out in paragraph 8.3. |
| **“CHECK Scheme”** | means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks |
| **“CHECK Service**  **Provider”** | means a company which, under the CHECK Scheme:   1. has been certified by the National Cyber Security   Centre;   1. holds “Green Light” status; and 2. is authorised to provide the IT Health Check services   required by paragraph 18 of the Security Requirements; |
| **“Code”** | means, in respect of the Developed System:   1. the source code; 2. the object code; 3. third-party components, including third-party coding frameworks and libraries; and **(d)** all supporting documentation. |
| **“Code Review”** | means a periodic review of the Code by manual or automated means to:   1. identify and fix any bugs; and 2. ensure the Code complies with:    1. the requirements of this Schedule [♦]   (*Security Management*); and   * 1. the Secure Development Guidance; |

|  |  |
| --- | --- |
| **“Code Review**  **Plan”** | means the document agreed with the Buyer under paragraph 9.3 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews; |
| **“Code Review**  **Report”** | means a report setting out the findings of a Code Review; |
| **“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; |
| **“Developed**  **System”** | means the software or system that the Supplier will develop under this Agreement; |
| **“Development**  **Activity”** | means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including:   1. coding; 2. testing; 3. code storage; and **(d)** deployment. |
| **“Development**  **Environment”** | means any information and communications technology system and the  Sites that the Supplier or its Sub-contractors will use to provide the Development Activity; |
| **“EEA”** | means the European Economic Area; |
| **“End-user Device”** | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services. |
| **“Email Service”** | means a service that will send, or can be used to send, emails from the  Buyer’s email address or otherwise on behalf of the Buyer; |
| “**HMG Baseline**  **Personnel Security**  **Standard**” | means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel  Standard”, Version 6.0, May 2018  (https://assets.publishing.service.gov.uk  /government/uploads/system/uploads/attachment\_data/file/714002/ HMG\_Baseline\_Personnel\_Security\_Standard\_-\_May\_2018.pdf), as that document is updated from time to time; |
| “**IT Health Check**” | means security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment in accordance with paragraph 33 of the Security Requirements; |
| “**Malicious**  **Software**” | means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, |

|  |  |
| --- | --- |
|  | data or other information, executable code, applications, macros or configurations; |
| “**Modules Register**” | means the register of Third-party Software Modules required for higher risk agreements by paragraph 11.3 of the Security Requirements; |
| “**NCSC**” | means the National Cyber Security Centre; |
| “**NCSC Cloud**  **Security**  **Principles**” | means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles. |
| “**NCSC Device**  **Guidance**” | means the NCSC’s document “Device Security Guidance”, as updated or replaced from time to time and found at  https://www.ncsc.gov.uk/collection/device-security-guidance; |
| “**NCSC Protecting**  **Bulk Personal Data**  **Guidance**” | means the NCSC’s document “Protecting Bulk Personal Data”, as updated or replaced from time to time and found at  https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data |
| “**NCSC Secure Design Principles”** | means the NCSC’s document “Secure Design Principles”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles. |
| “**OWASP**” | means the Open Web Application Security Project Foundation; |
| “**OWASP Secure Coding Practice**” | means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-referenceguide/migrated\_content; |
| “**OWASP Top Ten**” | means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/wwwproject-top-ten/; |
| “**Privileged User**” | means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges; |
| “**Process**” | means any operation 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 of that data; |
| “**Prohibited**  **Activity**” | means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice; |
| “**Prohibition**  **Notice**” | means a notice issued under paragraph 1.8 of the Security Requirements. |
| “**Protective Monitoring**  **System**” | means the system implemented by the Supplier and its Sub-contractors under paragraph 20.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code |

|  |  |
| --- | --- |
| “**Register of Support Locations and Third-Party**  **Tools**” | means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools:   1. the nature of the activity performed at the Support   Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable);   1. where that activity is performed by individuals, the place or facility from where that activity is performed; and 2. in respect of the entity providing the Support Locations or Third-Party Tools, its:    1. full legal name;    2. trading name (if any)    3. country of registration;    4. registration number (if applicable); and **(v)** registered address. |
| “**Relevant Activities**” | means those activities specified in paragraph 0 of the Security Requirements. |
| “**Relevant**  **Certifications**” | means   1. in the case of a standard agreement:    1. Cyber Essentials; and/or **(ii)** Cyber Essentials Plusas determined by the Buyer; or 2. in the case of a higher risk agreement:    1. ISO/IEC 27001:2013 by a UKAS-approved   certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and   * 1. Cyber Essentials Plus; |
| “**Relevant**  **Convictions**” | means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify |
| “**Remediation**  **Action Plan**” | means the plan prepared by the Supplier in accordance with  Paragraph 18.11 to 18.15, addressing the vulnerabilities and findings in a IT Health Check report |
| “**Secure**  **Development**  **Guidance**” | means:  **(a)** the NCSC’s document “Secure development and deployment guidance” as updated or replaced from time to time and found at  https://www.ncsc.gov.uk/collection/developers-collection; and |

|  |  |  |
| --- | --- | --- |
|  | **(b)** the OWASP Secure Coding Practice as updated or replaced from time to time; | |
| “**Security**  **Management Plan**” | means the document prepared in accordance with the requirements of Paragraph 9 and in the format, and containing the information, specified in Annex 2. | |
| “**SMP Subcontractor**” | means a Sub-contractor with significant market power, such that:   1. they will not contract other than on their own contractual terms; and 2. either:    1. there are no other substitutable suppliers of the particular services other than SMP Subcontractors; or    2. the Sub-contractor concerned has an effective monopoly on the provision of the Services. | |
| “**Sites**” | means any premises:   1. from or at which:    1. the Services are (or are to be) provided; or    2. the Supplier manages, organises or otherwise directs the provision or the use of the Services; or 2. where:    1. any part of the Supplier Information Management System is situated; or    2. any physical interface with the Buyer System takes place; and 3. for the avoidance of doubt include any premises at which Development Activities take place | |
| “**Sub-contractor**” | includes, for the purposes of this Schedule [♦] (*Security Management*), any individual or entity that:  **(a)** forms part of the supply chain of the Supplier; and | |
|  | **(b)** | has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data; |
| “**Sub-contractor**  **Personnel**” | means:  **(a)** | any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and |
|  | **(b)** | engaged in or likely to be engaged in:   1. the performance or management of the Services; 2. or the provision of facilities or services that are necessary for the provision of the Services. |
| “**Supplier**  **Information** | means: |  |

|  |  |
| --- | --- |
| **Management System**” | 1. those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; 2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and 3. for the avoidance of doubt includes the Development Environment. |
| “**Security Requirements**” | mean the security requirements in Annex 1 to this Schedule [♦] (*Security Management*) |
| “**Supplier**  **Personnel**” | means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Agreement; |
| “**Support Location**” | means a place or facility where or from which individuals may access or Process the Code or the Buyer Data; |
| “**Support Register**” | means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Agreements in accordance with paragraph 12 of the Security Requirements. |
| “**Third-party Software Module**” | means any module, library or framework that:   1. is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and 2. either:    1. forms, or will form, part of the Code; or    2. is, or will be, accessed by the Developed System during its operation. |
| “**Third-party Tool**” | means any activity conducted other than by the Supplier during which the Code or the Buyer Data is accessed, analysed or modified or some form of operation is performed on it; |
| “**UKAS**” | means the United Kingdom Accreditation Service; |

## 4 Introduction

4.1 This Schedule [♦] (*Security Management*) sets out:

1. the assessment of this Agreement as either a:
   1. higher risk agreement; or
   2. standard agreement, in Paragraph 1;
2. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of:
   1. the Development Activity;
   2. the Development Environment;
   3. the Buyer Data;
   4. the Services; and
   5. the Supplier Information Management System;
3. the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;
4. the Buyer’s access to the Supplier Personnel and Supplier Information Management System, in Paragraph 7;
5. the Certification Requirements, in Paragraph 8;
6. the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 9; and
7. the Security Requirements with which the Supplier and its Sub-contractors must comply.

## 5 Principles of Security

5.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data, and the integrity and availability of the Developed System, and, consequently, on the security of:

1. the Sites;
2. the Services; and
3. the Supplier’s Information Management System.
   1. The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 5.1.
   2. Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:
4. the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors;
5. the security and integrity of the Developed System; and
6. the security of the Supplier Information Management System.

5.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Subcontractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

## 6 Security Requirements

6.1 The Supplier shall:

1. comply with the Security Requirements; and
2. subject to Paragraph 6.2, ensure that all Sub-contractors also comply with the Security Requirements.

6.2 Where a Sub-contractor is SMP Sub-contractor, the Supplier shall:

1. use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;
2. document the differences between Security Requirements the obligations that the SMP Subcontractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;
3. take such steps as the Buyer may require to mitigate those risks.

## 7 Access to Supplier Personnel and Supplier Information Management System

7.1 The Buyer may require, and the Supplier must provide, and ensure that each Sub-contractor provides, the Buyer and its authorised representatives with:

1. access to the Supplier Personnel, including, for the avoidance of doubt, the Sub-contractor Personnel;
2. access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Subcontractor; and
3. such other information and/or documentation that the Buyer or its authorised representatives may require,

to allow the Buyer to audit the Supplier and its Sub-contractors’ compliance with this Schedule [] (*Security Management*) and the Security Requirements.

7.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 7.1: (a) in the case of a Breach of Security within 24 hours of such a request; and (b) in all other cases, within 10 Working Days of such request.

## 8 Certification Requirements

8.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, both:

1. it; and
2. any Sub-contractor,

is certified as compliant with the Relevant Certifications.

8.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:

1. the Relevant Certifications for it and any Sub-contractor; and
2. in the case of a higher-risk agreement, any relevant scope and statement of applicability required under the ISO/IEC 27001:2013 Relevant Certifications.

8.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:

1. currently in effect;
2. cover at least the full scope of the Supplier Information Management System; and
3. are not subject to any condition that may impact the provision of the Services or the Development Activity (the “**Certification Requirements**”).

8.4 The Supplier must notify the Buyer promptly, and in any event within three (3) Working Days, after becoming aware that, in respect of it or any Sub-contractor:

1. a Relevant Certification has been revoked or cancelled by the body that awarded it;
2. a Relevant Certification expired and has not been renewed by the Supplier;
3. a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or
4. the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”)

8.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 8.4:

1. the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 8.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Buyer setting out:
   1. full details of the Certification Default, including a root cause analysis;
   2. the actual and anticipated effects of the Certification Default;
   3. the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;
2. the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
3. if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working

Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph (b) will apply to the re-submitted plan;

1. the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;
2. if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

## 9 Security Management Plan

9.1 This Paragraph 9 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement.

*Preparation of Security Management Plan*

9.2 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule [♦] (*Security Management*) and the Agreement in order to ensure the security of the Development Environment, the Developed System, the Buyer Data and the Supplier Information Management System.

9.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, the Security Management Plan, which must include:

1. an assessment of the Supplier Information Management System against the requirements of this Schedule [♦] (*Security Management*), including the Security Requirements;
2. the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System. the Buyer Data, the Buyer, the Services and/or users of the Services; and
3. the following information, so far as is applicable, in respect of each Sub-contractor:

(i) the Sub-contractor’s:

* + - 1. legal name;
      2. trading name (if any);
      3. registration details (where the Sub-contractor is not an individual);
    1. the Relevant Certifications held by the Sub-contractor;
    2. the Sites used by the Sub-contractor;
    3. the Development Activity undertaken by the Sub-contractor;
    4. the access the Sub-contractor has to the Development Environment;
    5. the Buyer Data Processed by the Sub-contractor;
    6. the Processing that the Sub-contractor will undertake in respect of the Buyer Data;
    7. the measures the Sub-contractor has in place to comply with the requirements of this Schedule [***♦***] (*Security Management*);

1. the Register of Support Locations and Third Party Tools;
2. the Modules Register;
3. the Support Register;
4. details of the steps taken to comply with:
   * 1. the Secure Development Guidance; and
     2. the secure development policy required by the ISO/IEC 27001:2013 Relevant Certifications;
5. details of the protective monitoring that the Supplier will undertake in accordance with paragraph 20 of the Security Requirements, including:
6. the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System and the Development environment; and

(ii) the retention periods for audit records and event logs.

*Approval of Security Management Plan*

9.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

1. an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to:
   * 1. undertake the Development Activity; and/or
     2. Process Buyer Data; or
2. a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.
   1. If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.
   2. The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

*Updating Security Management Plan*

* 1. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

*Monitoring*

* 1. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

1. a significant change to the components or architecture of the Supplier Information Management System;
2. a new risk to the components or architecture of the Supplier Information Management System;
3. a vulnerability to the components or architecture of the Supplier Information Management

System using an industry standard vulnerability scoring mechanism;

1. a change in the threat profile;
2. a significant change to any risk component;
3. a significant change in the quantity of Personal Data held within the Service;
4. a proposal to change any of the Sites from which any part of the Services are provided; and/or
5. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

9.9 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

Annex 1 Security Requirements

## 1 Location

*Location for Relevant Activities*

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:

1. undertake the Development Activity;
2. host the Development Environment; and
3. store, access or process Buyer Data,

(the “**Relevant Activities**”) only in the geographic areas permitted by the Buyer.

1.2 Where the Buyer has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors undertake the Relevant Activities in a facility operated by an entity where:

1. the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
2. that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);
3. the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
4. the Supplier has provided the Buyer with such information as the Buyer requires concerning:
   * 1. the entity;
     2. the arrangements with the entity; and
     3. the entity’s compliance with the binding agreement; and
5. the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

1.3 Where the Supplier cannot comply with one or more of the requirements of paragraph 1.2: (a) it must provide the Buyer with such information as the Buyer requests concerning:

* + 1. the security controls in places at the relevant location or locations; and
    2. where certain security controls are not, or only partially, implemented the reasons for this;

1. the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
2. if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:
   * 1. cease to store, access or process Buyer Data at that location or those locations;
     2. sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or process Buyer Data at that location, or those locations, as the Buyer may specify.

*Support Locations*

* 1. The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.
  2. Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where:

1. the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
2. that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);
3. the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
4. the Supplier has provided the Authority with such information as the Authority requires concerning:
   * 1. the entity;
     2. the arrangements with the entity; and
     3. the entity’s compliance with the binding agreement; and
5. the Authority has not given the Supplier notice under paragraph 1.8.

*Third-party Tools*

* 1. The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.
  2. The Supplier must not, and must not allow Sub-contractors to, use a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

*Prohibited Activities*

* 1. The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a “**Prohibited Activity**”).

1. in any particular country or group of countries;
2. in or using facilities operated by any particular entity or group of entities; or
3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,

(a “**Prohibition Notice**”).

1.9 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Prohibited Activities affected by the notice, the Supplier must, and must procure that Subcontractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

## 2 Vetting, Training and Staff Access

*Vetting before performing or managing Services*

2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:

1. Development Activity;
2. any activity that provides access to the Development Environment; or (c) any activity relating to the performance and management of the Services unless:
3. that individual has passed the security checks listed in paragraph 2.2; or
4. the Buyer has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, the security checks are:

1. the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
   * 1. the individual’s identity;
     2. the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
     3. the individual’s previous employment history; and
     4. that the individual has no Relevant Convictions;
2. national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
3. such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

*Annual training*

2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

1. General training concerning security and data handling; and
2. Phishing, including the dangers from ransomware and other malware.

*Staff access*

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
  2. The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.
  3. Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel’s access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

*Exception for certain Sub-contractors*

* 1. Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

1. as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
2. provide such information relating to the Sub-contractor, its vetting processes and the roles

the affected Sub-contractor Personnel will perform as the Buyer reasonably requires; and

1. comply, at the Supplier’s cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

## 3 End-user Devices

3.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data or Code is stored or processed in accordance with the following requirements:

(a) the operating system and any applications that store, process or have access to Buyer Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications; (b) users must authenticate before gaining access;

1. all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;
2. 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;
3. 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 Buyer Data and Code to ensure the security of that Buyer Data and Code;
4. the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data or Code stored on the device and prevent any user or group of users from accessing the device;
5. all End-user Devices are within the scope of any Relevant Certification.
   1. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
   2. Where there is any conflict between the requirements of this Schedule [] (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

## 4 Secure Architecture

4.1 The Supplier shall design and build the Developed System in a manner consistent with:

1. the NCSC’s guidance on “Security Design Principles for Digital Services”;
2. where the Developed System will Process bulk data, the NCSC’s guidance on “Bulk Data Principles”; and
3. the NCSC’s guidance on “Cloud Security Principles”.

4.2 Where any of the documents referred to in paragraph 4.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

## 5 Secure Software Development by Design

5.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:

1. no malicious code is introduced into the Developed System or the Supplier Information Management System.
2. the Developed System can continue to function in accordance with the Specification:
   * 1. in unforeseen circumstances; and
     2. notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

5.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development

Activity:

1. comply with the Secure Development Guidance as if its requirements were terms of this Contract; and
2. document the steps taken to comply with that guidance as part of the Security Management Plan.

5.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development

Activity:

1. ensure that all Supplier Staff engaged in Development Activity are:
   1. trained and experienced in secure by design code development;
   2. provided with regular training in secure software development and deployment;
2. ensure that all Code:
   1. is subject to a clear, well-organised, logical and documented architecture;
   2. follows OWASP Secure Coding Practice
   3. follows recognised secure coding standard, where one is available;
   4. employs consistent naming conventions;
   5. is coded in a consistent manner and style;
   6. is clearly and adequately documented to set out the function of each section of code;
   7. is subject to appropriate levels of review through automated and non-automated methods both as part of:

(A) any original coding; and (B) at any time the Code is changed;

1. ensure that all Development Environments:
   1. protect access credentials and secret keys;
   2. are logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;
   3. require multi-factor authentication to access;
   4. have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;
   5. use network architecture controls to constrain access from the Development

Environment to the Developed System or the Supplier Information Management System;

## 6 Code Repository and Deployment Pipeline

1. The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:
   1. when using a cloud-based code depository for the deployment pipeline, use only a cloud-based code depository that has been assessed against the NCSC Cloud Security Principles;
   2. ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
   3. ensure secret credentials are separated from source code.
   4. run automatic security testing as part of any deployment of the Developed System.

## 8 Development and Testing Data

8.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing, .

## 9 Code Reviews

9.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

9.2 The Supplier must:

1. regularly; or
2. as required by the Buyer review the Code in accordance with the requirements of this paragraph 9 (a “**Code Review**”).

9.3 Before conducting any Code Review, the Supplier must agree with the Buyer:

1. the modules or elements of the Code subject to the Code Review;
2. the development state at which the Code Review will take place;
3. any specific security vulnerabilities the Code Review will assess; and
4. the frequency of any Code Reviews (the “**Code Review Plan**”).
   1. For the avoidance of doubt, the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.
   2. The Supplier:
5. must undertake Code Reviews in accordance with the Code Review Plan; and
6. may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.
   1. No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the Code Review Report.
   2. Where the Code Review identifies any security vulnerabilities, the Supplier must:
7. remedy these at its own cost and expense;
8. ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and
9. modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and
10. provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 9.7.

## 10 Third-party Software

10.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Process the Buyer Data greater than those rights strictly necessary for the use of the software.

## 11 Third-party Software Modules

11.1 This paragraph 11 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement

11.2 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:

1. verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
2. perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;
3. continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;
4. take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
   1. The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the “**Modules Register**”).
   2. The Modules Register must include, in respect of each Third-party Software Module:
5. full details of the developer of the module;
6. the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;
7. any recognised security vulnerabilities in the Third-party Software Module; and
8. how the Supplier will minimise the effect of any such security vulnerability on the Developed System.

11.5 The Supplier must:

1. review and update the Modules Register:
   1. within 10 Working Days of becoming aware of a security vulnerability in any Thirdparty Software Module; and
   2. at least once every 6 (six) months;
2. provide the Buyer with a copy of the Modules Register: (i) whenever it updates the Modules Register; and

(ii) otherwise when the Buyer requests.

## 12 Hardware and software support

12.1 This paragraph 12 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement

12.2 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

12.3 The Supplier must produce and maintain a register of all software that form the Supplier Information Management System (the “**Support Register**”).

12.4 The Support Register must include in respect of each item of software:

1. the date, so far as it is known, that the item will cease to be in mainstream security support; and
2. the Supplier’s plans to upgrade the item before it ceases to be in mainstream security support.

12.5 The Supplier must:

1. review and update the Support Register:
   * 1. within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;
     2. within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and
     3. at least once every 12 (twelve) months;
2. provide the Buyer with a copy of the Support Register: (i) whenever it updates the Support Register; and

(ii) otherwise when the Buyer requests.

12.6 Where any element of the Developed System consists of COTS Software, the Supplier shall ensure:

1. those elements are always in mainstream or extended security support from the relevant vendor; and
2. the COTS Software is not more than one version or major release behind the latest version of the software.

12.7 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:

1. regular firmware updates to the hardware; and
2. a physical repair or replacement service for the hardware.

## 13 Encryption

13.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

13.2 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods

that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 13.

13.3 Where this paragraph 13 requires Buyer Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under paragraph 13.2.

13.4 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that the Developed System encrypts Buyer Data:

(a) when the Buyer Data is stored at any time when no operation is being performed on it; and (b) when the buyer Data is transmitted.

13.5 Unless paragraph 13.6 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:

1. when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
2. when transmitted.

13.6 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 13.5, the Supplier must:

1. immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
3. provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
   1. The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
   2. Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
4. the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
5. the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.

13.9 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].

## 14 Email

14.1 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that where the Developed System will provide an Email Service to the Buyer, the Developed System:

1. supports transport layer security (“**TLS**”) version 1.2, or higher, for sending and receiving emails;
2. supports TLS Reporting (“**TLS-RPT**”);
3. is capable of implementing:
   1. domain-based message authentication, reporting and conformance (“**DMARC**”);
   2. sender policy framework (“**SPF**”); and
   3. domain keys identified mail (“**DKIM**”); and
4. is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:
   1. the UK Government (current version at https://www.gov.uk/guidance/set-upgovernment-email-services-securely; or
   2. the NCSC (current version at https://www.ncsc.gov.uk/collection/email-security-andanti-spoofing).

## 15 DNS

15.1 Unless otherwise agreed by the Buyer, the Supplier must ensure that the Developed System uses the UK public sector Protective DNS (“**PDNS**”) service to resolve internet DNS queries.

## 16 Malicious Software

16.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.

16.2 The Supplier must ensure that such Anti-virus Software:

1. prevents the installation of the most common forms of Malicious Software in the Supplier

Information Management System and the Development Environment;

1. is configured to perform automatic software and definition updates;
2. provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update’s release by the vendor;
3. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
4. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
   1. 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 Buyer Data, assist each other to mitigate any [Losses] and to restore the Services to their desired operating efficiency.

* 1. The Supplier must at all times, during and after the [Term], on written demand indemnify the Buyer

and keep the Buyer indemnified, against all [Losses] incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this paragraph .

## 17 Vulnerabilities

17.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:

1. seven (7) days after the public release of patches for vulnerabilities classified as “critical”;
2. thirty (30) days after the public release of patches for vulnerabilities classified as “important”; and
3. sixty (60) days after the public release of patches for vulnerabilities classified as “other”.

17.2 The Supplier must:

1. scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and
2. if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with paragraph 17.1.

17.3 For the purposes of this paragraph 17, the Supplier must implement a method for classifying

vulnerabilities to the Supplier Information Management System as “critical”, “important” or “other” that is aligned to recognised vulnerability assessment systems, such as:

1. the National Vulnerability Database’s vulnerability security ratings; or
2. Microsoft’s security bulletin severity rating system.

## 18 Security testing

*Responsibility for security testing*

18.1 The Supplier is solely responsible for:

1. the costs of conducting any security testing required by this Paragraph 18 (unless the Buyer gives notice under Paragraph 18.2); and
2. the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

*Security tests by Buyer*

* 1. The Buyer may give notice to the Supplier that the Buyer will undertake the security testing required by Paragraph 18.4(a) and 18.4(d).
  2. Where the Buyer gives notice under Paragraph 18.2:

1. the Supplier shall provide such reasonable co-operation as the Buyer requests, including:
   * 1. such access to the Supplier Information Management System as the Buyer may request; and
     2. such technical and other information relating to the Information Management System as the Buyer requests;
2. the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and
3. for the purposes of Paragraphs 18.8 to 18.17:
   * 1. the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and
     2. the time limits in Paragraphs 18.8 and 18.11 run from the date on which the Buyer provides the Supplier with the copy of the report under Paragraph (b). *Security tests by Supplier*

18.4 The Supplier must:

1. during the testing of the Developed System and before the Developed System goes live

(unless the Buyer gives notice under Paragraph 18.2);

1. at least once during each [Contract Year]; and (c) when required to do so by the Buyer; undertake the following activities:
2. conduct security testing of the Developed System and the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an “**IT Health Check**”) in accordance with Paragraph 18.5 to 18.7; and
3. implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 18.8 to 18.17.

*IT Health Checks*

18.5 In arranging an IT Health Check, the Supplier must:

1. use only a CHECK Service Provider to perform the IT Health Check;
2. design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.
3. promptly provide the Buyer with such technical and other information relating to the

Information Management System as the Buyer requests;

1. include within the scope of the IT Health Check such tests as the Buyer requires;
2. agree with the Buyer the scope, aim and timing of the IT Health Check.
   1. The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.
   2. Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

*Remedying vulnerabilities*

* 1. In addition to complying with Paragraphs 18.4 to 18.17, the Supplier must remedy:

1. any vulnerabilities classified as critical in the IT Health Check report within 5 Working Days of becoming aware of the vulnerability and its classification;
2. any vulnerabilities classified as high in the IT Health Check report within 1 month of becoming aware of the vulnerability and its classification; and
3. any vulnerabilities classified as medium in the IT Health Check report within 3 months of becoming aware of the vulnerability and its classification.
   1. The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in the IT Health Check report within the time periods specified in Paragraph 18.8.

*Significant vulnerabilities*

* 1. Where the IT Health Check report identifies more than 10 vulnerabilities classified as either critical or high, the Buyer may, at the Supplier’s cost, appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities.

*Responding to an IT Health Check report*

* 1. Where the IT Health Check identifies vulnerabilities in, or makes findings in respect of, the

Information Management System, the Supplier must within 20 Working Days of receiving the IT Health Check report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the “**Remediation Action Plan**”).

* 1. Where the Buyer has commissioned a root cause analysis under Paragraph 18.10, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.
  2. The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the IT Health Check report:

1. how the vulnerability or finding will be remedied;
2. the date by which the vulnerability or finding will be remedied; and
3. the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.
   1. The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.
   2. The Buyer may:
4. reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:
   * 1. the Supplier shall within 10 Working Days of the date on which the Buyer rejected

the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer’s reasons; and

* + 1. paragraph 18.13 to 18.15 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;

1. accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 18.16 and 18.17.

*Implementing an approved Remediation Action Plan*

* 1. In implementing the Remediation Action plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.
  2. If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

1. provide the Buyer with a full, unedited and unredacted copy of the test report;
2. implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;
3. as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

## 19 Access Control

19.1 This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk agreement.

19.2 The Supplier must, and must ensure that all Sub-contractors:

1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
2. require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
4. maintain records detailing each person’s access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

19.3 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:

1. are allocated to a single, individual user;
2. are accessible only from dedicated End-user Devices;
3. are configured so that those accounts can only be used for system administration tasks;
4. require passwords with high complexity that are changed regularly;
5. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and
6. in the case of a higher-risk agreement are:
   * 1. restricted to a single role or small number of roles;
     2. time limited; and
     3. restrict the Privileged User’s access to the internet.
   1. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.
   2. The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.
   3. The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 19.2 to 19.5.
   4. The Supplier must, and must ensure that all Sub-contractors:
7. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
8. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

## 20 Event logging and protective monitoring

*Protective Monitoring System*

20.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports analysing access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code to:

1. identify and prevent potential Breaches of Security;
2. respond effectively and in a timely manner to Breaches of Security that do occur;
3. identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and
4. help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the “**Protective Monitoring System**”).

20.2 The Protective Monitoring System must provide for:

1. event logs and audit records of access to the Supplier Information Management system; and
2. regular reports and alerts to identify:
   * 1. changing access trends;
     2. unusual usage patterns; or
     3. the access of greater than usual volumes of Buyer Data;
3. the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;
4. any other matters required by the Security Management Plan.

*Event logs*

20.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log: (a) personal data, other than identifiers relating to users; or

(b) sensitive data, such as credentials or security keys.

*Provision of information to Buyer*

20.4 The Supplier must provide the Buyer on request with:

1. full details of the Protective Monitoring System it has implemented; and
2. copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

*Changes to Protective Monitoring System*

20.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to:

1. respond to a specific threat identified by the Buyer;
2. implement additional audit and monitoring requirements; and
3. stream any specified event logs to the Buyer’s security information and event management system.

## 21 Audit rights

*Right of audit*

21.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:

1. verify the Supplier’s or Sub-contractor’s (as applicable) compliance with the requirements of this Schedule [] (*Security Management*) and the Data Protection Laws as they apply to Buyer Data;
2. inspect the Supplier Information Management System (or any part of it); (c) review the integrity, confidentiality and security of the Buyer Data; and/or

(d) review the integrity and security of the Code.

21.2 Any audit undertaken under this Paragraph 21:

1. may only take place during the Term and for a period of 18 months afterwards; and
2. is in addition to any other rights of audit the Buyer has under this Agreement.

21.3 The Buyer may not undertake more than one audit under Paragraph 21.1 in each calendar year unless the Buyer has reasonable grounds for believing:

1. the Supplier or any Sub-contractor has not complied with its obligations under this

Agreement or the Data Protection Laws as they apply to the Buyer Data;

1. there has been or is likely to be a Security Breach affecting the Buyer Data or the Code; or
2. where vulnerabilities, or potential vulnerabilities, in the Code have been identified by: (i) an IT Health Check; or

(ii) a Breach of Security.

*Conduct of audits*

* 1. The Authority must use reasonable endeavours to provide 15 Working Days’ notice of an audit.
  2. The Authority must when conducting an audit:

1. comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Suppler Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and
2. use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

21.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all cooperation and assistance the Buyer may reasonably require, including:

1. all information requested by the Buyer within the scope of the audit;
2. access to the Supplier Information Management System; and
3. access to the Supplier Staff.

*Response to audit findings*

21.7 Where an audit finds that:

1. the Supplier or a Sub-contractor has not complied with this Agreement or the Data

Protection Laws as they apply to the Buyer Data; or

1. there has been or is likely to be a Security Breach affecting the Buyer Data

the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

21.8 The exercise by the Buyer of any rights it may have under this Paragraph 3 does not affect the exercise by it of any other or equivalent rights it may have under this Agreement in respect of the audit findings.

## 22 Breach of Security

*Reporting Breach of Security*

22.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

*Immediate steps*

22.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other steps reasonably necessary to:

1. minimise the extent of actual or potential harm caused by such Breach of Security;
2. remedy such Breach of Security to the extent possible;
3. apply a tested mitigation against any such Breach of Security; and
4. prevent a further Breach of Security in the future which exploits the same root cause failure;

*Subsequent action*

22.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:

1. full details of the Breach of Security; and
2. if required by the Buyer:
   * 1. a root cause analysis; and
     2. a draft plan addressing the root cause of the Breach of Security

(the “**Breach Action Plan**”).

22.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause analysis:

1. how the issue will be remedied;
2. the date by which the issue will be remedied; and
3. the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.
   1. The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.
   2. The Buyer may:
4. reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:
   * 1. the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer’s reasons; and
     2. paragraph 22.5 and 22.6 shall apply to the revised draft Breach Action Plan;
5. accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

*Assistance to Buyer*

* 1. Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must provide such assistance to the Buyer as the Buyer requires until the Breach of

Security and any impacts or potential impacts on the Buyer are resolved to the Buyer’s satisfaction.

* 1. The obligation to provide assistance under Paragraph 22.7 continues notwithstanding the expiry or termination of this Contract.

*Reporting of Breach of Security to regulator*

* 1. Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:

1. make that report within the time limits:
   * 1. specified by the relevant regulator; or
     2. otherwise required by Law;
2. to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.

22.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:

1. provide such information and other input as the Buyer requires within the timescales specified by the Buyer;
2. where Paragraph 7 applies to the Breach of Security, ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

## 23 Return and Deletion of Buyer Data

23.1 The Supplier must create and maintain a register of:

1. all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and
2. those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Subcontractor, on which the Buyer Data is stored (the “**Buyer Data Register**”).

23.2 The Supplier must:

1. review and update the Buyer Data Register:
   * 1. within 10 Working Days of the Supplier or any Sub-contractor changes to those parts of the Supplier Information Management System on which the Buyer Data is stored;
     2. within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;
     3. at least once every 12 (twelve) months; and
2. provide the Buyer with a copy of the Buyer Data Register: (i) whenever it updates the Buyer Data Register; and

(ii) otherwise when the Buyer requests.

23.3 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

1. when requested to do so by the Buyer; and
2. using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

23.4 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

1. when requested to do so by the Buyer; and
2. using the method specified by the Buyer.

Annex 2 Security Management Plan

[***Insert template for Security Management Plan***]

## Order Schedule 10 (Exit Management)

### 1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **"Exclusive Assets"** | Supplier Assets used exclusively by the Supplier or a Key Subcontractor in the provision of the Deliverables; |
| **"Exit Information"** | has the meaning given to it in Paragraph 3.1 of this Schedule; |
| **"Exit Manager"** | the person appointed by each Party to manage their respective obligations under this Schedule; |
| **“Exit Plan”** | the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule; |
| **"Net Book Value"** | the current net book value of the relevant Supplier Asset(s) calculated in accordance with the DPS Application or Order Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice); |
| **"Non-Exclusive Assets"** | those Supplier Assets used by the Supplier or a Key Subcontractor in connection with the Deliverables but which are also used by the Supplier or Key Subcontractor for other purposes; |
| **"Registers"** | the register and configuration database referred to in Paragraph 2.2 of this Schedule; |
| **"Replacement Goods"** | any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Replacement Services"** | any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, |
|  | whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Termination Assistance"** | the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice; |
| **"Termination Assistance**  **Notice"** | has the meaning given to it in Paragraph  5.1 of this Schedule; |
| **"Termination Assistance**  **Period"** | the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule; |
| **"Transferable Assets"** | Exclusive Assets which are capable of legal transfer to the Buyer; |
| **"Transferable Contracts"** | Sub-Contracts, licences for Supplier's  Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in  relation to licences all relevant  Documentation; |
| **"Transferring Assets"** | has the meaning given to it in Paragraph  8.2.1 of this Schedule; |
| **"Transferring Contracts"** | has the meaning given to it in Paragraph 8.2.3 of this Schedule. |

### 2. Supplier must always be prepared for contract exit

2.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Subcontracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables ("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

### 3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier’s or its Subcontractors’ prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

### 4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in

Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier’s staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

1. every six (6) months throughout the Contract Period; and
2. no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;
3. as soon as reasonably possible following a

Termination Assistance Notice, and in any event no

later than ten (10) Working Days after the date of the Termination Assistance Notice;

1. as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

* 1. Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
  2. A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

### 5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination

Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

### 6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI’s) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

### 7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

1. such information relating to the Deliverables as remains in the possession or control of the Supplier; and
2. such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

### 8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**"); 8.2.2 which, if any, of:

1. the Exclusive Assets that are not Transferable Assets; and
2. the Non-Exclusive Assets, the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring**

**Contracts"**), in order for the Buyer and/or its Replacement Supplier to provide the

Deliverables from the expiry of the Termination Assistance Period. The

Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which

Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

* 1. With effect from the expiry of the Termination Assistance Period, the

Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

* 1. Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
  2. Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-

Exclusive Assets, the Supplier shall as soon as reasonably practicable:

* + 1. procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
    2. procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
  1. The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
  2. The Buyer shall:
     1. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
     2. once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
  3. The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.
  4. The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

### 9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

### 10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

**Order Schedule 14 (Service Levels)**

## 1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

1

**“Critical Service** 2 has the meaning given to it in the Order Form; **Level Failure”**

**"Service Credits"** 3 any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;

**"Service Credit** 4 has the meaning given to it in the Order Form; **Cap"**

**"Service Level** 5 means a failure to meet the Service Level

**Failure"** Performance Measure in respect of a Service Level;

**"Service Level** 6 shall be as set out against the relevant Service

**Performance** Level in the Annex to Part A of this Schedule; and **Measure"**

**"Service Level** 7 shall be as set out against the relevant Service **Threshold"** Level in the Annex to Part A of this Schedule.

## 2. What happens if you don’t meet the Service Levels

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to meet any Service Level Performance Measure.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 A Service Credit shall be the Buyer’s exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

1. exceeds the relevant Service Level Threshold;
2. has arisen due to a Prohibited Act or wilful Default by the Supplier;
3. results in the corruption or loss of any Government Data; and/or
4. results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months’ notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

* + 1. the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
    2. the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
    3. there is no change to the Service Credit Cap.

## 3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that

Service Period ("**Compensation for Critical Service Level Failure**"), provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

**Part A: Service Levels and Service Credits**

## 1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

## 2. Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

**Annex A to Part A: Services Levels and Service Credits Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service Levels | |  |  | Service Credit for each Service Period |
| Service  Level  Performance  Criterion | Key  Indicator | Service Level  Performance  Measure | Service  Level  Threshold |
| **[**Accurate and timely billing of  Buyer | Accuracy  /Timelines | at least 98% at all times | [ ] | 0.5% Service  Credit gained for  each percentage under the specified Service Level  Performance  Measure |
| Access to Buyer support | Availability | at least 98% at all times | [ ] | 0.5% Service  Credit gained for  each percentage under the specified Service Level  Performance  Measure |

The Service Credits shall be calculated on the basis of the following formula:

[Example:

Formula: x% (Service Level

Performance Measure) - x% (actual Service Level performance)

= x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Worked example: 98% (e.g.

Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period)

= 23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer]

**Part B: Performance Monitoring**

## 3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

3.2.3 details of any Critical Service Level Failures;

3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

3.2.6 such other details as the Buyer may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The

Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

3.3.2 be attended by the Supplier's Representative and the Buyer’s Representative; and

3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer’s Representative and any other recipients agreed at the relevant meeting.

3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer’s Representative at each meeting.

3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

## 4. Satisfaction Surveys

4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

**Order Schedule 15 (Order Contract Management)**

## 1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

**"Operational Board"** the board established in accordance with paragraph 2.1 of this Schedule;

**"Project Manager"** the manager appointed in accordance with paragraph

2.1 of this Schedule;

## 2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

## 3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager shall be:

3.1.1 the primary point of contact to receive communication from the

Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be the delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager by the

Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

## 4. Role of the Operational Board

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member’s attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier’s performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

## 5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Order Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks; 5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Order Contract which the Buyer and the Supplier have identified.

**Order Schedule 18 (Background Checks)** Order Ref:

Crown Copyright 2021

**Order Schedule 18 (Background Checks)**

1. **When you should use this Schedule**

This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

1. **Definitions**

**“Relevant Conviction”** means any conviction listed in Annex 1 to this Schedule.

1. **Relevant Convictions** 
   1. The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.
   2. Notwithstanding Paragraph 3.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

(a) carry out a check with the records held by the Department for Education (DfE); (b) conduct thorough questioning regarding any Relevant

Convictions; and

(c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and

Barring Service (DBS), and the Supplier shall not (and shall ensure that any Subcontractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

DPS Ref: RM6219 Learning and Training

Project Version: v1.0 1

Model Version: v1.0

**Order Schedule 18 (Background Checks)**

Order Ref:

Crown Copyright 20

21

DPS Ref: RM6219 Learning and Training

Project Version:

v1.0

2

Model Version: v1.0

**Annex 1**

**–**

**Relevant Convictions**

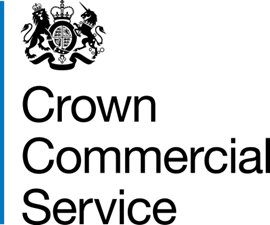
**[**

**Insert**

Relevant Convictions here]

**Commented [HK1]:**

Hi Riz, can you fill this in



**Order Schedule 20 (Order Specification)**

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract

**CONTENTS**

[1. PURPOSE 3](#_Toc265893)

[2. BACKGROUND TO THE CONTRACTING AUTHORITY 3](#_Toc265894)

[3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT 3](#_Toc265895)

[4. DEFINITIONS 4](#_Toc265896)

[5. SCOPE OF REQUIREMENT 4](#_Toc265897)

[6. THE REQUIREMENT 5](#_Toc265898)

[7. KEY MILESTONES AND DELIVERABLES 7](#_Toc265899)

[8. MANAGEMENT INFORMATION/REPORTING 8](#_Toc265900)

[9. CONTINUOUS IMPROVEMENT 8](#_Toc265901)

[10. SUSTAINABILITY 9](#_Toc265902)

[11. QUALITY 9](#_Toc265903)

[12. PRICE 9](#_Toc265904)

[13. STAFF AND CUSTOMER SERVICE 9](#_Toc265905)

[14. SECURITY AND CONFIDENTIALITY REQUIREMENTS ................................................ 9](#_Toc265906)

[15. PAYMENT AND INVOICING 11](#_Toc265907)

[16. LOCATION 11](#_Toc265908)

# 1. PURPOSE

1.1 The Government Communication Service (GCS) requires an external Supplier with the expertise, capability and successful experience in developing and maintaining digital learning platforms.

1.2 The Supplier will support the delivery of our GCS Advance Programme by supporting development and maintaining our dedicated edX instance in an AWS environment that allows us to offer our users a seamless service whilst maintaining robust security and data protection.

1.3 The supplier will support integrations between our edX instance and other platforms designed to improve management of the Advance programme and scaling of digital learning courses to new markets.

# 2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Cabinet Office is the centre of the UK Government. Its purpose is to:

support the Prime Minister and Cabinet to deliver the Government’s programme; drive efficiencies and reforms that will make Government work better; create a more united democracy; and strengthen and secure the United Kingdom at home and abroad.

2.2 GCS is the professional body for people working in communication roles across Government, and the international capability-building unit within GCS is called GCSI. Its aim is to deliver world-class communications that support Ministers' priorities, improve people's lives and enable the effective operation of our public service. It serves both politicians and the public alike.

# 3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 GCS has been building its Digital Learning capability over the last few years. To deliver digital learning effectively at scale, GCS must be able to offer courses online via a high quality digital platform. Our current offering is built using an instance of edX, a massive open online course (MOOC) provider that supports open source development. To maintain the service to users we need support in maintaining, integrating and updating our edX instance and related components that make up our learning platform.

3.2 The service comprises an Open edX application. Extensions have been developed for a custom theme, enhancements to the API and improvements to the Gradebook.

3.3 An administration service for user and course booking management (GCAS\*) has also been built in Python Django, with a MySQL database for data storage. The supplier would also need to be able to support, develop and integrate with GCAS.

3.4 A focus will be placed in the coming months on deepening integrations between EdX and the GCS platform for member services, GCS Connect. Integrations with include creating automated and dynamic learner records, tracking completion of L&D and ensuring Single Sign On (SSO) between the two platforms is maintained.

3.5 The services have been built using an infrastructure as code (IaC) approach with GitHub Actions, Terraform and Helm and deployed to a Kubernetes (EKS) based AWS platform with multiple environments such as Development, Test, Staging and Production.

3.6 The service is expected to see an average annual usage of approximately 7,000 users.

# 4. DEFINITIONS

|  |  |
| --- | --- |
| **Expression or Acronym** | **Definition** |
| SaS | Skills and Standards |
| GCS | Government Communication Service |
| GCSU | Government Curriculum and Skills Unit |
| GCAS | Global Communications Academy System (the system commissioned by the Government Communications Academy) |
| GCS Connect | The membership platform which will house user data and allow learners to display their learner record. |
| GCS Advance | Is the new L&D programme for Government  Communication Service members in the UK public sector. |
| Practitioner | The digital learning led L&D offer of GCS Advance. |
| Leader | The in person offer for senior leaders |
| Expert | The in person offer for managers and deep discipline experts |
| EdX | The learning platform used by GCS. |
| CO | Cabinet Office or the Contracting Authority |
| CDIO | Central Digital and Information Office within Cabinet Office |

# 5. SCOPE OF REQUIREMENT

5.1 GCS requires a Supplier to provide continuous Support, Maintenance and Development for our digital learning platform edX.

5.2 GCS requires a ‘Partner’ to help deliver and Support delivery of the GCS Advance Programme.

5.3 GCS will require bidders to provide a summary of their proposed delivery approach, as well as details of their experience working with edX in other comparable learning contexts.

5.4 Bidders should include a portfolio of credentials outlining their evidence of past project delivery in this field within their tender proposals.

# 6. THE REQUIREMENT

### 6.1 Billing

6.1.1 The Supplier shall provide a monthly billing report and the following months forecast on a monthly basis.

### 6.2 Collaboration

6.2.1 The Supplier must be able to work with the CO CDIO team and other CO stakeholders whenever any compatibility changes are needed to our centrally held AWS account or for the purposes of integrations with other government platforms.

6.2.2 The Supplier shall actively participate in Agile meetings (such as stand-ups, retrospectives, show and tells etc)

6.2.3 The Supplier shall agree on the team members allocated to the project. The GCS SaS Team expect to use a "One Team" approach to delivery, with supplier development staff also available to the CO Team for communications.

6.2.4 The Supplier shall continue to deliver post the Full Launch to deliver on the Authorities priorities as set out in the Backlog

6.2.5 The Supplier shall demonstrate how it would propose to work with the Authority to deliver its backlog.

6.2.6 The Supplier shall have a flexible approach to working with CO, with an openness to co-creation.

6.2.7 The Supplier shall support the Authority in its story and backlog refinement and estimations (T-Shirt sizing)

6.2.8 The Supplier shall use the tools and processes for delivery as agreed with GCS.

6.2.9 The Supplier shall work through the Development and management of an evolving backlog

6.2.10 The Supplier shall work with the Authority and its Suppliers to ensure all milestones are met in item 7.1 (Milestone Worksheet)

6.2.11 The Supplier shall work with the Authority to support development activity for the delivery of a Practitioner Pilot Programme in September 2023 and the Full Launch of Practitioner Programme in

April 2024

6.2.12 The Supplier should allow the CO Team to interact directly with all staff working on the project.

### 6.3 Documentation

6.3.1 The Supplier should create or maintain comprehensive documentation, including user manuals, system architecture, API documentation, and any other relevant technical documentation when making changes to the system

### 6.4 Integration

6.4.1 The Supplier must be able to handle integration across multiple fields (name, grade, department etc) and be flexible in adding new fields as needed.

6.4.2 The Supplier must Implement integration between data held in GCS Connect or GCSU platforms and either the EdX LMS or GCAS booking system with the intention of simplifying the learner registration process and to ensure the learner record in GCS Connect is updated automatically on completion of courses.

6.4.3 The supplier shall implement changes to the booking system to ensure added flexibility of the automated email system.

6.4.4 The Supplier should allow Learners to receive notifications and updates regarding course enrolments, deadlines, announcements, and any changes to the course content.

6.4.5 The supplier shall implement changes to the booking system so that new registrants on courses can be stopped at a certain number or by a certain date.

6.4.6 The Supplier should allow the front end (landing page) to enable learners to enrol on courses directly from the front-end interface, seamlessly initiating the enrolment process in the respective learning portals.

6.4.7 The Supplier must implement a functioning data dashboard for GCS team to interpret and gain insight from.

6.4.8 The Supplier should allow Administrators to have access to customisable reports and analytics dashboards for monitoring the performance and effectiveness of the integrated learning portals.

6.4.9 The Supplier should allow the front end (landing page) to provide comprehensive reporting and analytics features to track learner progress, course completion rates, assessment scores, and other relevant metrics.

6.4.10 The Supplier will create and maintain integration with existing CO and Supplier Systems (such as Civil Service Learning, Government Skills Campus Omniplex etc), using standard protocols or APIs to enable MI collection and reporting.

6.4.11 The Supplier must allow Interoperability with other LMS solutions across government such as Government Commercial College, Civil Service Learning & Government Campus Online.

6.4.12 The Supplier will create and maintain integration with existing CO and Supplier Systems (such as Connect, Government Skills Campus, Civil Service Learning, Omniplex etc), using standard protocols or APIs to enable a seamless user experience.

### 6.5 Maintenance

6.5.1 The Supplier will be responsible for providing 24x7 technical support for the LMS according to mutually agreed SLAs.

6.5.2 The Supplier should provide ongoing technical support, bug fixes, and regular updates for the front-end system, ensuring its smooth operation and compatibility with future changes in the integrated learning portals.

6.5.3 When available, the Supplier schedule ensure the LMS receives periodic and timely software upgrades from Open EdX on a mutually agreed schedule.

### 6.6 Scalability

6.6.1 The Supplier shall ensure that the LMS is scalable and able to handle approximately 20,000 learners and 3,000 concurrent user sessions without compromising performance.

6.6.2 The Supplier should conduct performance testing to ensure the front end can efficiently handle the data retrieval and processing from multiple back-end systems.

6.6.3 The Supplier will setup new LMS environments as required by GCS to provide either testing environments or the means to ensure courses are available to multiple audiences.

### 6.7 Security

6.7.1 The Supplier shall ensure that the LMS will adhere to GCS and CDO data privacy regulations, such as GDPR, ensuring user consent and the handling of personal data.

6.7.2 The Supplier shall ensure that the LMS will adhere to GCS and CDO security practices to protect user data, including encryption of sensitive information and secure transmission of data between the front end and back-end systems.

### 6.8 Technical Capability

6.8.1 The Supplier should have strong visual design capability, specifically UX capability.

6.8.2 The Supplier will have an iterative, test-and-learn approach to design and production and experience in designing to meet user needs.

6.8.3 The Supplier will demonstrate technical capability sufficient to maintain and improve on our current operational platform (including experience of AWS services, utilising a Kubernetes containerised environment, Open edX) A full list of core capabilities required can be provided upon request.

6.8.4 The Supplier will provide development resources to support a range of requests. The type of requests could include: edX version upgrades, additional functionality requests to gradebook or other bespoke aspects, configuration requests (e.g. integrating H5P), improvement of usability and UI of edX components, data aggregation and analysis.

### 6.9 Accessibility

6.9.1 The Supplier will ensure the platform offers a simple and intuitive user journey, in order to be accessible to different cultural audiences and across different languages, considering all levels of digital skills and experience.

6.9.2 The Supplier will ensure the platform supports industry and WCAG 2.2 standards of accessibility across global markets through a range of electronic devices including mobiles, tablets, laptops and desktops. It will need to be compatible with a variety of internet browsers, mobile and tablet devices globally. Governments often use outdated browsers and this will need to be accounted for.

# 7. KEY MILESTONES AND DELIVERABLES

7.1 The following Contract milestones/deliverables shall apply:

|  |  |
| --- | --- |
| **Milestone/Deliverable** | **Timeframe or Delivery Date** |
| Maintain operability and improvements to new learner dashboard via Open API | April 2024 onwards |
| Ensure EdX version updates happen on an agreed regular schedule | Throughout |
| Complete Beta launch of commercialised digital learning offer through EdX, including public facing front end | March 2025 |
| Support integration with new Government Skills Campus to ensure automated updates to civil service learner records | March 2025 |

# 8. MANAGEMENT INFORMATION/REPORTING

8.1 The Supplier will report to a named day-to-day CO lead.

8.2 A project delivery team drawn from CO and including the project manager and team as needed from the Supplier will meet regularly, at least once a week, including frequent face-to-face/video call working sessions.

# 9. CONTINUOUS IMPROVEMENT

9.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

9.2 The Supplier should present new ways of working to the Authority during quarterly Contract review meetings.

9.3 The Supplier and GCS will work in accordance with the principles of Agile development. The Supplier will have an iterative, test-and-learn approach to design and production and a knowledge of how to design to meet user needs.

9.4 Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

# 10. SUSTAINABILITY

10.1 Products should be developed with due regard to environmental impact, diversity and equality within the [UK sustainability goals.](https://www.gov.uk/government/publications/implementing-the-sustainable-development-goals/implementing-the-sustainable-development-goals--2)

# 11. QUALITY

11.1 The Supplier will adhere to Digital Learning standards and Accessibility guidelines outlined in the [GDS Service Manual.](https://www.gov.uk/service-manual)

11.2 The Supplier will adhere to user requirements as identified in any user testing by CO.

11.3 The Supplier will adhere to style guidelines as supplied by CO.

11.4 All content is to be approved by CO before being released.

11.5 The technical platform must facilitate the moderation of user-generated content (e.g. discussion boards) by CO at a local and global level.

# 12. PRICE

12.1 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

12.2 The Supplier will provide the total price of the contract to meet the requirement.

# 13. STAFF AND CUSTOMER SERVICE

13.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

13.2 The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

13.3 The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

# 14. SECURITY AND CONFIDENTIALITY REQUIREMENTS

14.1 Suppliers must have appropriate and documented IT, physical, personnel and procedural security measures in place to prevent any unauthorised access to, or leakage of data and to prevent it being shared with any unauthorised third parties.

### 14.2 Certification Requirements

14.2.1 The Supplier must have a current and valid Cyber Essentials Plus Certificate awarded by one of the Government approved Cyber Essentials accreditation bodies within the last 12 months (see: https://www.gov.uk/government/publications/cyber-essentialsscheme-overview) and/or a current and valid ISO 27001:2013

Certification, or be willing to obtain one of these certifications within three months of contract award.

### 14.3 Patching and Penetration Testing/IT Health Checks

14.3.1 The Supplier must proactively monitor Supplier vulnerability websites and demonstrate the ability to ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the Cloud Security Principles [https://www.ncsc.gov.uk/guidance/implementing-cloud-securityprinciples](https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles)

14.3.2 The Supplier must undertake the following security assurance activities at their own cost and expense to demonstrate that the people, processes, technical and physical controls have been delivered in an effective way.

14.3.3 Penetration testing to be carried out by certified CREST or CHECK supplier, within 3 months of Contract Award.

14.3.4 Penetration testing of the production environment must be done before any Authority data is stored or processed on the platform.

14.3.5 The penetration testing scope must include any devices used to manage the solution.

14.3.6 An annual penetration test must be undertaken with the scope agreed with the Authority and when there is a significant change to the infrastructure/service,

14.3.7 After receiving the penetration testing report, the full report must be shared with the Authority and the Supplier must produce a remediation plan to agreed timescales which must be agreed with the Authority.

### 14.4 Physical Security

14.4.1 On physical security, the Supplier must have appropriate physical security measures in place in any data centres used to host the Authority’s data and should describe in detail what those measures are.

### 14.5 Personnel Security

14.5.1 Potential Providers will ensure all staff have undergone preemployment checks to a minimum of the Government Baseline Personnel Security Standard (or equivalent).

### 14.6 Risk Management Documentation

14.6.1 The successful Supplier will prepare a Risk Management Document (a template will be provided by the Authority), which details the information assurance and security controls applied to the delivery of the solution. This will include how the Supplier is meeting the Cloud Security Principles: [https://www.ncsc.gov.uk/guidance/implementing-cloud-securityprinciples](https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles)

14.6.2 The Supplier will need to keep this document updated to reflect the current security position at least annually during the life of the contract.

### 14.7 Protective Monitoring

14.7.1 The Supplier must ensure that they have a protective monitoring solution and regime in place at all times and must be able to provide evidence of such.

### 14.8 General Data Protection Regulation (GDPR) Compliance

14.8.1 Full compliance with the GDPR and any other applicable data protection laws is essential, with the Authority being the Data Controller and the Supplier being the Data Processor.

### 14.9 Third Party Suppliers

14.9.1 Any Third Party Suppliers involved in the delivery of the solution must meet with the certification requirements at 15.1 unless agreed otherwise by the authority.

### 14.10 Incident Reporting

14.10.1 Any security incidents relevant to the solution must be reported to an agreed point of contact within the Authority within two working days.

# 15. PAYMENT AND INVOICING

15.1 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

15.2 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

15.3 Invoices should be submitted to: TBC AT AWARD

15.4 Attendance at Contract Review meetings shall be at the Supplier’s own expense.

# 16. LOCATION

16.1 The location of the Services will be carried out at United Kingdom and Bogota, Columbia.

**Joint Schedule 1 (Definitions)**

1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint 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 each 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 Central Government 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;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

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 each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

1.3.12 in entering into a Contract the Relevant Authority is acting as part of the Crown; and

1.3.13 any reference in a Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

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 Exit 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
2. any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

|  |  |
| --- | --- |
| **"Achieve"** | in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and "**Achieved**", "**Achieving**" and "**Achievement**" shall be construed accordingly; |
| **"Additional**  **Insurances"** | insurance requirements relating to an Order Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements); |
| **"Admin Fee”** | means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-amsupplier/management-information/admin-fees; |
| **"Affected Party"** | the Party seeking to claim relief in respect of a Force Majeure Event; |
| **"Affiliates"** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time; |
| **“Annex”** | extra information which supports a Schedule; |
| **"Approval"** | the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly; |
| **"Audit"** | the Relevant Authority’s right to:  a) verify the accuracy of the Charges and any other amounts payable by a Buyer under an Order Contract (including proposed or actual variations to them in accordance with the Contract); |

|  |  |
| --- | --- |
|  | 1. verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; 2. verify the Open Book Data; 3. verify the Supplier’s and each Subcontractor’s compliance with the Contract and applicable Law; 4. identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; 5. identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any   Subcontractors or their ability to provide the Deliverables;   1. obtain such information as is necessary to fulfil the Relevant Authority’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; 2. review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; 3. carry out the Relevant Authority’s internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; 4. enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant   Authority has used its resources; or   1. verify the accuracy and completeness of any Management   Information delivered or required by the DPS Contract; |
| **"Auditor"** | 1. the Relevant Authority’s internal and external auditors; 2. the Relevant Authority’s statutory or regulatory auditors; 3. the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; 4. HM Treasury or the Cabinet Office; 5. any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and 6. successors or assigns of any of the above; |
| **"Authority"** | CCS and each Buyer; |
| **"Authority Cause"** | any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant |

|  |  |
| --- | --- |
|  | Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier; |
| **"BACS"** | the Bankers’ Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom; |
| **"Beneficiary"** | a Party having (or claiming to have) the benefit of an indemnity under this Contract; |
| **"Buyer"** | the relevant public sector purchaser identified as such in the Order Form; |
| **"Buyer Assets"** | the Buyer’s infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract; |
| **"Buyer Authorised**  **Representative"** | the representative appointed by the Buyer from time to time in relation to the Order Contract initially identified in the Order Form; |
| **"Buyer Premises"** | premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them); |
| **"CCS"** | the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP; |
| **"CCS Authorised**  **Representative"** | the representative appointed by CCS from time to time in relation to the DPS Contract initially identified in the DPS Appointment Form and subsequently on the Platform; |
| **"Central**  **Government**  **Body"** | 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:   1. Government Department; 2. Non-Departmental Public Body or Assembly Sponsored Public   Body (advisory, executive, or tribunal);   1. Non-Ministerial Department; or 2. Executive Agency; |
| **"Change in Law"** | any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date; |
| **"Change of**  **Control"** | a change of control within the meaning of Section 450 of the Corporation Tax Act 2010; |
| **"Charges"** | the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Order Contract, as set out in the Order Form, |

|  |  |
| --- | --- |
|  | for the full and proper performance by the Supplier of its obligations under the Order Contract less any Deductions; |
| **"Claim"** | any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract; |
| **"Commercially**  **Sensitive**  **Information"** | the Confidential Information listed in the DPS Appointment Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss; |
| **"Comparable**  **Supply"** | the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables; |
| **"Compliance**  **Officer"** | the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations; |
| **"Confidential**  **Information"** | means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential; |
| **"Conflict of**  **Interest"** | a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS; |
| **"Contract"** | either the DPS Contract or the Order Contract, as the context requires; |
| **"Contract Period"** | the term of either a DPS Contract or Order Contract on and from the earlier of the:   1. applicable Start Date; or 2. the Effective Date up to and including the applicable End Date; |
| **"Contract Value"** | the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier; |
| **"Contract Year"** | a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof; |
| **"Control"** | control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly; |
| **“Controller”** | has the meaning given to it in the UK GDPR; |
| **“Core Terms”** | CCS’ terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under DPS Contracts and Order Contracts; |

|  |  |
| --- | --- |
| **"Costs"** | the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:   1. the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including:   i) base salary paid to the Supplier Staff; ii) employer’s National Insurance contributions; iii) pension contributions; iv) car allowances;   * 1. any other contractual employment benefits;   2. staff training; vii) work place accommodation; viii)work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and   ix) reasonable recruitment costs, as agreed with the Buyer;   1. costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the   Supplier in respect of those Supplier Assets;   1. operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and 2. Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any   Deliverables; but excluding:   1. Overhead; 2. financing or similar costs; 3. maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Order Contract Period whether in relation to Supplier Assets or otherwise; 4. taxation; 5. fines and penalties; 6. amounts payable under Order Schedule 16 (Benchmarking) where such Schedule is used; and |

|  |  |
| --- | --- |
|  | o) non-cash items (including depreciation, amortisation, impairments and movements in provisions); |
| **"CRTPA"** | the Contract Rights of Third Parties Act 1999; |
| **“Data Protection Impact**  **Assessment”** | an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| **"Data Protection**  **Legislation"** | (i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy; |
| **“Data Protection**  **Liability Cap”** | the amount specified in the DPS Appointment Form; |
| **"Data Protection**  **Officer"** | has the meaning given to it in the UK GDPR; |
| **"Data Subject"** | has the meaning given to it in the UK GDPR; |
| **"Data Subject**  **Access Request"** | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |
| **"Deductions"** | all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under an Order Contract; |
| **"Default"** | any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority; |
| **"Default**  **Management Levy"** | has the meaning given to it in Paragraph 8.1.1 of DPS Schedule 5 (Management Levy and Information); |
| **"Delay Payments"** | the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan; |
| **"Deliverables"** | Goods and/or Services that may be ordered under the Contract including the Documentation; |
| **"Delivery"** | delivery of the relevant Deliverable or Milestone in accordance with the terms of an Order Contract as confirmed and accepted by the Buyer by either (a) confirmation in writing to the Supplier; or (b) where Order Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly; |

|  |  |
| --- | --- |
| **"Disclosing Party"** | the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential); |
| **"Dispute"** | any claim, dispute or difference (whether contractual or noncontractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may  successfully be brought in the English courts; |
| **"Dispute**  **Resolution**  **Procedure"** | the dispute resolution procedure set out in Clause 34 (Resolving disputes); |
| **"Documentation"** | descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:   1. would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables 2. is required by the Supplier in order to provide the Deliverables; and/or 3. has been or shall be generated for the purpose of providing the Deliverables; |
| **"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; |
| **“DPA 2018”** | the Data Protection Act 2018; |
| **“DPS”** | the dynamic purchasing system operated by CCS in accordance with Regulation 34 that this DPS Contract governs access to; |
| **"DPS Application"** | the application submitted by the Supplier to CCS and annexed to or referred to in DPS Schedule 2 (DPS Application); |
| **"DPS Appointment**  **Form"** | the document outlining the DPS Incorporated Terms and crucial information required for the DPS Contract, to be executed by the Supplier and CCS and subsequently held on the Platform; |
| **"DPS Contract"** | the dynamic purchasing system access agreement established between CCS and the Supplier in accordance with Regulation 34 |

|  |  |
| --- | --- |
|  | by the DPS Appointment Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service; |
| **"DPS Contract**  **Period"** | the period from the DPS Start Date until the End Date of the DPS Contract; |
| **"DPS Expiry Date"** | the date of the end of the DPS Contract as stated in the DPS Appointment Form; |
| **"DPS Incorporated**  **Terms"** | the contractual terms applicable to the DPS Contract specified in the DPS Appointment Form; |
| **"DPS Initial**  **Period"** | the initial term of the DPS Contract as specified in the DPS Appointment Form; |
| **"DPS Optional**  **Extension Period"** | such period or periods beyond which the DPS Initial Period may be extended as specified in the DPS Appointment Form; |
| **"DPS Pricing"** | the maximum price(s) applicable to the provision of the Deliverables set out in DPS Schedule 3 (DPS Pricing); |
| **"DPS**  **Registration"** | the registration process a Supplier undertakes when submitting its details onto the Platform; |
| **"DPS SQ**  **Submission"** | the Supplier’s selection questionnaire response; |
| **"DPS Special**  **Terms"** | any additional terms and conditions specified in the DPS Appointment Form incorporated into the DPS Contract; |
| **"DPS Start Date"** | the date of start of the DPS Contract as stated in the DPS Appointment Form; |
| **"Due Diligence**  **Information"** | any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date; |
| **“Effective Date”** | the date on which the final Party has signed the Contract; |
| **"EIR"** | the Environmental Information Regulations 2004; |
| **“Electronic**  **Invoice”** | an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870; |
| **"Employment**  **Regulations"** | the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC; |
| **"End Date"** | the earlier of:   1. the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or 2. if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract; |

|  |  |
| --- | --- |
| **"Environmental**  **Policy"** | to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer; |
| **"Equality and**  **Human Rights**  **Commission"** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **“Estimated Year 1**  **Contract Charges”** | the anticipated total charges payable by the Supplier in the first Contract Year specified in the Order Form; |
| **“Estimated Yearly**  **Charges”** | means for the purposes of calculating each Party’s annual liability under clause 11.2 :   1. in the first Contract Year, the Estimated Year 1 Contract Charges; or      1. in any subsequent Contract Years, the Charges paid or payable in the previous Contract Year; or iii) after the end of the Contract, the Charges paid or payable in the last Contract Year during the Contract Period; |
| **"Existing IPR"** | any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise); |
| **“Exit Day”** | shall have the meaning in the European Union (Withdrawal) Act 2018; |
| **"Expiry Date"** | the DPS Expiry Date or the Order Expiry Date (as the context dictates); |
| **"Extension**  **Period"** | the DPS Optional Extension Period or the Order Optional Extension Period as the context dictates; |
| **"Filter Categories"** | the number of categories specified in DPS Schedule 1  (Specification), if applicable; |
| **"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 relevant Government department in relation to such legislation; |
| **"Force Majeure**  **Event"** | any event outside the reasonable control of either Party affecting its performance of its obligations under the 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:  a) riots, civil commotion, war or armed conflict; |

|  |  |
| --- | --- |
|  | 1. acts of terrorism; 2. acts of government, local government or regulatory bodies; 3. fire, flood, storm or earthquake or other natural disaster,   but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor'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; |
| **"General Anti-**  **Abuse Rule"** | 1. the legislation in Part 5 of the Finance Act 2013; and 2. any future legislation introduced into parliament to counteract Tax advantages arising from abusive arrangements to avoid National Insurance contributions; |
| **"General Change in Law"** | a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply; |
| **"Goods"** | goods made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form ; |
| **"Good Industry**  **Practice"** | standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector; |
| **"Government"** | 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 other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| **"Government**  **Data"** | the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority’s Confidential Information, and which:   1. are supplied to the Supplier by or on behalf of the Authority; or 2. the Supplier is required to generate, process, store or transmit pursuant to a Contract; |
| **"Guarantor"** | the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract; |
| **"Halifax Abuse**  **Principle"** | the principle explained in the CJEU Case C-255/02 Halifax and others; |

|  |  |
| --- | --- |
| **"HMRC"** | Her Majesty’s Revenue and Customs; |
| **"ICT Policy"** | the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Order Start Date (a copy of which has been supplied to the  Supplier), as updated from time to time in accordance with the Variation Procedure; |
| **"Impact**  **Assessment"** | an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:   1. details of the impact of the proposed Variation on the   Deliverables and the Supplier's ability to meet its other obligations under the Contract;   1. details of the cost of implementing the proposed Variation; 2. details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the DPS Pricing/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; 3. a timetable for the implementation, together with any proposals for the testing of the Variation; and 4. such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request; |
| **"Implementation**  **Plan"** | the plan for provision of the Deliverables set out in Order Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer; |
| **"Indemnifier"** | a Party from whom an indemnity is sought under this Contract; |
| **“Independent**  **Control”** | where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and  “**Independent Controller**” shall be construed accordingly; |
| **"Indexation"** | the adjustment of an amount or sum in accordance with DPS Schedule 3 (DPS Pricing) and the relevant Order Form; |
| **"Information"** | has the meaning given under section 84 of the Freedom of Information Act 2000; |
| **"Information Commissioner"** | the UK’s independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies; |
| **"Initial Period"** | the initial term of a Contract specified on the Platform or the Order Form, as the context requires; |
| **"Insolvency**  **Event"** | with respect to any person, means: |

|  |  |
| --- | --- |
|  | (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:   1. (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 2. (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986; 3. 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; 4. 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; 5. 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 14 days; 6. that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business; 7. where that person is a company, a LLP or a partnership: 8. a petition is presented (which is not dismissed within 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; 9. 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; 10. (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 11. (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; |
| **"Installation**  **Works"** | all works which the Supplier is to carry out at the beginning of the Order Contract Period to install the Goods in accordance with the Order Contract; |
| **"Intellectual Property Rights" or "IPR"** | 1. copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information; 2. 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 3. all other rights having equivalent or similar effect in any country or jurisdiction; |
| **"Invoicing**  **Address"** | the address to which the Supplier shall invoice the Buyer as specified in the Order Form; |
| **"IPR Claim"** | any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract; |
| **"IR35"** | the off-payroll rules requiring individuals who work through their company pay the same income tax and National Insurance contributions as an employee which can be found online at:  https://www.gov.uk/guidance/ir35-find-out-if-it-applies; |
| **“Joint Controller**  **Agreement”** | the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (*Processing Data*); |
| **“Joint**  **Controllers”** | where two or more Controllers jointly determine the purposes and means of Processing; |
| **"Key Staff"** | the individuals (if any) identified as such in the Order Form; |
| **"Key Sub-**  **Contract"** | each Sub-Contract with a Key Subcontractor; |
| **"Key**  **Subcontractor"** | any Subcontractor:   1. which is relied upon to deliver any work package within the   Deliverables in their entirety; and/or   1. which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or |

|  |  |
| --- | --- |
|  | q) 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 the Order  Contract, and the Supplier shall list all such Key Subcontractors on the Platform and in the Key Subcontractor Section in the Order Form; |
| **"Know-How"** | all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party’s possession before the applicable Start Date; |
| **"Law"** | any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply; |
| **"Losses"** | all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly; |
| **"Management**  **Information" or “MI”** | the management information specified in DPS Schedule 5 (Management Levy and Information); |
| **"Management**  **Levy"** | the sum specified on the Platform payable by the Supplier to CCS in accordance with DPS Schedule 5 (Management Levy and  Information); |
| **“MI Default”** | means whentwo (2) MI Reports are not provided in any rolling six  (6) month period |
| **"MI Failure"** | means when an MI report:   1. contains any material errors or material omissions or a missing mandatory field; or 2. is submitted using an incorrect MI reporting Template; or 3. is not submitted by the reporting date (including where a declaration of no business should have been filed); |
| **"MI Report"** | means a report containing Management Information submitted to the Authority in accordance with DPS Schedule 5 (Management Levy and Information); |
| **"MI Reporting**  **Template"** | means the form of report set out in the Annex to DPS Schedule 5 (Management Levy and Information) setting out the information the  Supplier is required to supply to the Authority; |
| **"Milestone"** | an event or task described in the Implementation Plan; |
| **"Milestone Date"** | the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved; |

|  |  |
| --- | --- |
| **"Month"** | a calendar month and "**Monthly**" shall be interpreted accordingly; |
| **"National**  **Insurance"** | contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004); |
| **"New IPR"** | 1. IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or 2. IPR in or arising as a result of the performance of the Supplier’s obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier’s Existing IPR; |
| **"Occasion of Tax**  **Non–Compliance"** | where:   1. 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 in any jurisdiction 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 in any jurisdiction; and/or   1. any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which 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 Start Date or to a civil penalty for fraud or evasion; |
| **"Open Book Data**  **"** | complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Order Contract, including details and all assumptions relating to: y) the Supplier’s Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;  z) operating expenditure relating to the provision of the Deliverables including an analysis showing:  i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; |

|  |  |
| --- | --- |
|  | 1. staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade; 2. a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and 3. Reimbursable Expenses, if allowed under the Order Form;   aa) Overheads; bb) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;   1. the Supplier Profit achieved over the DPS Contract Period and on an annual basis; 2. confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; 3. an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and ff) the actual Costs profile for each Service Period; |
| **"Order"** | means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract; |
| **"Order Contract"** | the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the DPS Contract), which consists of the terms set out and referred to in the Order Form; |
| **"Order Contract**  **Period"** | the Contract Period in respect of the Order Contract; |
| **"Order Expiry**  **Date"** | the date of the end of an Order Contract as stated in the Order Form; |
| **"Order Form"** | a completed Order Form Template (or equivalent information issued by the Buyer) used to create an Order Contract; |
| **"Order Form**  **Template"** | the template in DPS Schedule 6 (Order Form Template and Order Schedules); |
| **"Order**  **Incorporated Terms"** | the contractual terms applicable to the Order Contract specified under the relevant heading in the Order Form; |
| **"Order Initial**  **Period"** | the Initial Period of an Order Contract specified in the Order Form; |
| **"Order Optional**  **Extension Period"** | such period or periods beyond which the Order Initial Period may be extended as specified in the Order Form; |
| **"Order Procedure"** | the process for awarding an Order Contract pursuant to Clause 2 (How the contract works) and DPS Schedule 7 (Order Procedure); |

|  |  |
| --- | --- |
| **"Order Special**  **Terms"** | any additional terms and conditions specified in the Order Form incorporated into the applicable Order Contract; |
| **"Order Start Date"** | the date of start of an Order Contract as stated in the Order Form; |
| **"Order Tender"** | the tender submitted by the Supplier in response to the Buyer’s Statement of Requirements following an Order Procedure and set out at Order Schedule 4 (Order Tender); |
| **"Other**  **Contracting**  **Authority"** | any actual or potential Buyer under the DPS Contract; |
| **"Overhead"** | those amounts which are intended to recover a proportion of the Supplier’s or the Key Subcontractor’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 Staff and accordingly included within limb (a) of the definition of "Costs"; |
| **"Parliament"** | takes its natural meaning as interpreted by Law; |
| **"Party"** | in the context of the DPS Contract, CCS or the Supplier, and in the in the context of an Order Contract the Buyer or the Supplier.  "**Parties**" shall mean both of them where the context permits; |
| **"Performance**  **Indicators" or "PIs"** | the performance measurements and targets in respect of the Supplier’s performance of the DPS Contract set out in DPS Schedule 4 (DPS Management); |
| **"Personal Data"** | has the meaning given to it in the UK GDPR; |
| **“Personal Data**  **Breach”** | has the meaning given to it in the UK GDPR; |
| **“Personnel”** | all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract; |
| **“Platform”** | the online application operated on behalf of CCS to facilitate the technical operation of the DPS; |
| **"Prescribed**  **Person"** | a legal adviser, an MP or an appropriate body which a whistleblower may make a disclosure to as detailed in ‘Whistleblowing: list of prescribed people and bodies’, 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-thewhistle-list-of-prescribed-people-and-bodies--2/whistleblowing-listof-prescribed-people-and-bodies; |
| **“Processing”** | has the meaning given to it in the UK GDPR; |
| **“Processor”** | has the meaning given to it in the UK GDPR; |
| **"Progress**  **Meeting"** | a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative; |

|  |  |
| --- | --- |
| **"Progress Meeting**  **Frequency"** | the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form; |
| **“Progress Report”** | a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates; |
| **“Progress Report**  **Frequency”** | the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form; |
| **“Prohibited Acts”** | 1. to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:    1. induce that person to perform improperly a relevant function   or activity; or   * 1. reward that person for improper performance of a relevant function or activity;  1. 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 each Contract; or 2. committing any offence:    1. under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or    2. under legislation or common law concerning fraudulent acts; or    3. defrauding, attempting to defraud or conspiring to defraud a   Buyer or other public body; or jj) 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 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 the such measures adopted by it including those outlined in DPS Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the DPS Contract or Order Schedule 9 (Security), if applicable, in the case of an Order Contract; |
| **“Recall”** | a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance; |

|  |  |
| --- | --- |
| **"Recipient Party"** | the Party which receives or obtains directly or indirectly Confidential Information; |
| **"Rectification**  **Plan"** | the Supplier’s plan (or revised plan) to rectify it’s breach using the template in Joint Schedule 10 (Rectification Plan) which shall include:   1. full details of the Default that has occurred, including a root cause analysis; 2. the actual or anticipated effect of the Default; and 3. the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable); |
| **"Rectification Plan**  **Process"** | the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process); |
| **"Regulations"** | the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires); |
| **"Reimbursable**  **Expenses"** | the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:  nn) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the  Buyer otherwise agrees in advance in writing; and oo) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed; |
| **"Relevant**  **Authority"** | the Authority which is party to the Contract to which a right or obligation is owed, as the context requires; |
| **"Relevant**  **Authority's**  **Confidential**  **Information"** | pp) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New  IPR); qq) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority’s attention or into the Relevant Authority’s possession in connection with a Contract; and information derived from any of the above; |

|  |  |
| --- | --- |
| **"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 pursuant to section 9 of the Bribery Act 2010; |
| **"Relevant Tax**  **Authority"** | HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established; |
| **"Reminder Notice"** | a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time; |
| **"Replacement**  **Deliverables"** | any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Order Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Replacement**  **Subcontractor"** | a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor); |
| **"Replacement**  **Supplier"** | any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer; |
| **"Request For**  **Information"** | a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs; |
| **"Required**  **Insurances"** | the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form; |
| **"Satisfaction**  **Certificate"** | the certificate (materially in the form of the document contained in Part B of Order Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Order Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test; |
| **"Security**  **Management Plan"** | the Supplier's security management plan prepared pursuant to Order Schedule 9 (Security) (if applicable); |
| **"Security Policy"** | the Buyer's security policy, referred to in the Order Form, in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier; |
| **"Self Audit**  **Certificate"** | means the certificate in the form as set out in DPS Schedule 8 (Self Audit Certificate); |
| **"Serious Fraud**  **Office"** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **“Service Levels”** | any service levels applicable to the provision of the Deliverables under the Order Contract (which, where Order Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule); |

|  |  |
| --- | --- |
| **"Service Period"** | has the meaning given to it in the Order Form; |
| **"Services"** | services made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form; |
| **"Service Transfer"** | any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor; |
| **"Service Transfer**  **Date"** | the date of a Service Transfer; |
| **"Sites"** | any premises (including the Buyer Premises, the Supplier’s premises or third party premises) from, to or at which:  rr) the Deliverables are (or are to be) provided; or ss) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; |
| **"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 enterprises; |
| **"Special Terms"** | any additional Clauses set out in the DPS Appointment Form or Order Form which shall form part of the respective Contract; |
| **"Specific Change in Law"** | a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date; |
| **"Specification"** | the specification set out in DPS Schedule 1 (Specification), as may, in relation to an Order Contract, be supplemented by the Order Form; |
| **"Standards"** | any:   1. standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; 2. standards detailed in the specification in DPS Schedule 1   (Specification); vv) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;  ww) relevant Government codes of practice and guidance applicable from time to time; |

|  |  |
| --- | --- |
| **"Start Date"** | in the case of the DPS Contract, the date specified on the DPS Appointment Form, and in the case of an Order Contract, the date specified in the Order Form; |
| **"Statement of**  **Requirements"** | a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Order Procedure; |
| **"Storage Media"** | the part of any device that is capable of storing and retrieving data; |
| **"Sub-Contract"** | any contract or agreement (or proposed contract or agreement), other than an Order Contract or the DPS Contract, pursuant to which a third party:   1. provides the Deliverables (or any part of them); 2. provides facilities or services necessary for the provision of the   Deliverables (or any part of them); and/or zz) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them); |
| **"Subcontractor"** | any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person; |
| **"Subprocessor"** | any third party appointed to process Personal Data on behalf of that Processor related to a Contract; |
| **"Supplier"** | the person, firm or company identified in the DPS Appointment Form; |
| **"Supplier Assets"** | all assets and rights used by the Supplier to provide the Deliverables in accordance with the Order Contract but excluding the Buyer Assets; |
| **"Supplier**  **Authorised**  **Representative"** | the representative appointed by the Supplier named in the DPS Appointment Form, or later defined in an Order Contract; |
| **"Supplier's**  **Confidential**  **Information"** | 1. any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; 2. any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier’s attention or into the Supplier’s possession in connection with a Contract; ccc) Information derived from any of (a) and (b) above; |
| **"Supplier's Contrac**  **t**  **Manage**  **r”** | the person identified in the Order Form appointed by the Supplier to oversee the operation of the Order Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment; |

|  |  |
| --- | --- |
| **"Supplier Equipment"** | the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Order Contract; |
| **"Supplier**  **Marketing**  **Contact"** | shall be the person identified in the DPS Appointment Form; |
| **"Supplier Non-**  **Performance"** | where the Supplier has failed to:   1. Achieve a Milestone by its Milestone Date; 2. provide the Goods and/or Services in accordance with the   Service Levels ; and/or fff) comply with an obligation under a Contract; |
| **"Supplier Profit"** | in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of an Order Contract for the relevant period; |
| **"Supplier Profit**  **Margin"** | in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage; |
| **"Supplier Staff"** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under a Contract; |
| **“Supply Chain Information**  **Report Template”** | the document at Annex 1 of Joint Schedule 12 (Supply Chain  Visibility); |
| **"Supporting**  **Documentation"** | sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Order Contract detailed in the information are properly payable; |
| **“Tax”** | ggg) all forms of taxation whether direct or indirect; hhh) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;   1. all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and 2. any penalty, fine, surcharge, interest, charges or costs relating to any of the above,   in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction; |

|  |  |
| --- | --- |
| **"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 a Contract on a specified date and setting out the grounds for termination; |
| **"Test Issue"** | any variance or non-conformity of the Deliverables from their requirements as set out in an Order Contract; |
| **"Test Plan"** | a plan:   1. for the Testing of the Deliverables; and 2. setting out other agreed criteria related to the achievement of Milestones; |
| **"Tests "** | any tests required to be carried out pursuant to an Order Contract as set out in the Test Plan or elsewhere in an Order Contract and "**Tested**" and “**Testing**” shall be construed accordingly; |
| **"Third Party IPR"** | Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables; |
| **"Transferring**  **Supplier**  **Employees"** | those employees of the Supplier and/or the Supplier’s Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date; |
| **"Transparency**  **Information"** | the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for –   1. any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and 2. Commercially Sensitive Information; |
| **"Transparency**  **Reports"** | the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Order Schedule 1 (Transparency Reports); |
| **"UK GDPR"** | the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **"Variation"** | any change to a Contract; |
| **"Variation Form"** | the form set out in Joint Schedule 2 (Variation Form); |
| **"Variation Procedure"** | the procedure set out in Clause 24 (Changing the contract); |
| **"VAT"** | value added tax in accordance with the provisions of the Value Added Tax Act 1994; |
| **"VCSE"** | a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives; |
| **"Worker"** | any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note  08/15 (Tax Arrangements of Public Appointees)  (https://www.gov.uk/government/publications/procurement-policynote-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; |
| **"Working Day"** | any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form; |
| **"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; and |
| **"Work Hours"** | the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks. |

**Joint Schedule 2 (Variation Form)**

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Contract Details** | | |
| This variation is between: | "**CCS”**  And  **[insert** name of Supplier**]** (**"the Supplier"**) | | |
| Contract name: | **RM6219 DPS Agreement** **(“the Contract”)** | | |
| Contract reference number: |  | | |
|  | **Details of Proposed Variation** | | |
| Variation initiated by: | CCS | | |
| Variation number: | **001** | | |
| Date variation is raised: | **9th September 2022** | | |
| Proposed variation | To remove the current restriction and allow Suppliers to utilise SubContractors when providing Standard Off The Shelf Training. | | |
| Reason for the variation: | During our preliminary market consultations for the Learning & Training Services DPS, the general consensus received from SMEs indicated a preference to provide Standard Off The Shelf Training directly without having to be part of a Prime Vendor’s Supply Chain, so the use of subcontractors was not permitted for this service type.  However, following recent engagement with newly appointed suppliers since the launch of the DPS, it has become apparent that the use of Subcontractors is standard within the training market, even amongst SMEs who subcontract with each other and this restriction is also precluding other SMEs applying to join the DPS. | | |
| An Impact Assessment shall be provided within: | **5** days | | |
|  | **Impact of Variation** | | |
| Likely impact of the proposed variation: |  | **[Supplier to insert** | assessment of impact] |
|  |
|  | **Outcome of Variation** | | |
| Contract variation: | This Contract detailed above is varied as follows:  The Specification currently reads as follows:  Standard Off-The-Shelf Training  *○ Off-the-shelf training courses and professional qualifications, that are only provided by the training provider (no aggregators / sub-contractors).*    The Specification to be altered as follows:  Standard Off-The-Shelf Training | | |

Project Version: v2.0

Model Version: v1.0

Crown Copyright 2021

|  |  |  |
| --- | --- | --- |
|  | ○ *Off-the-shelf training courses and professional qualifications” as part of the proposed variation.* | |
| Financial variation: | Original Contract Value: | £ **0** |
| Additional cost due to variation: | £ **0** |
| New Contract value: | £0 |

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by CCS
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Project Version: v2.0

Model Version: v1.0

Crown Copyright 2021

Signed by an authorised signatory for and on behalf of the CCS

|  |  |
| --- | --- |
| Signature  Date  Name (in Capitals) Address |  |
|  |
|  |
|  |
|  |

Signed by an authorised signatory to sign for and on behalf of the Supplier

|  |  |
| --- | --- |
| Signature  Date  Name (in Capitals)  Address |  |
|  |
|  |
|  |

Project Version: v2.0

Model Version: v1.0

**Joint Schedule 3 (Insurance Requirements)**

## 1. The insurance you need to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under an Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") 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:

1.1.1 the DPS Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Order Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (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;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

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

## 2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables 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;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 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. What happens if you aren’t insured

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

## 4. Evidence of insurance you must provide

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

## 5. Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

## 6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or nonrenewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

## 7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables 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 Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

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

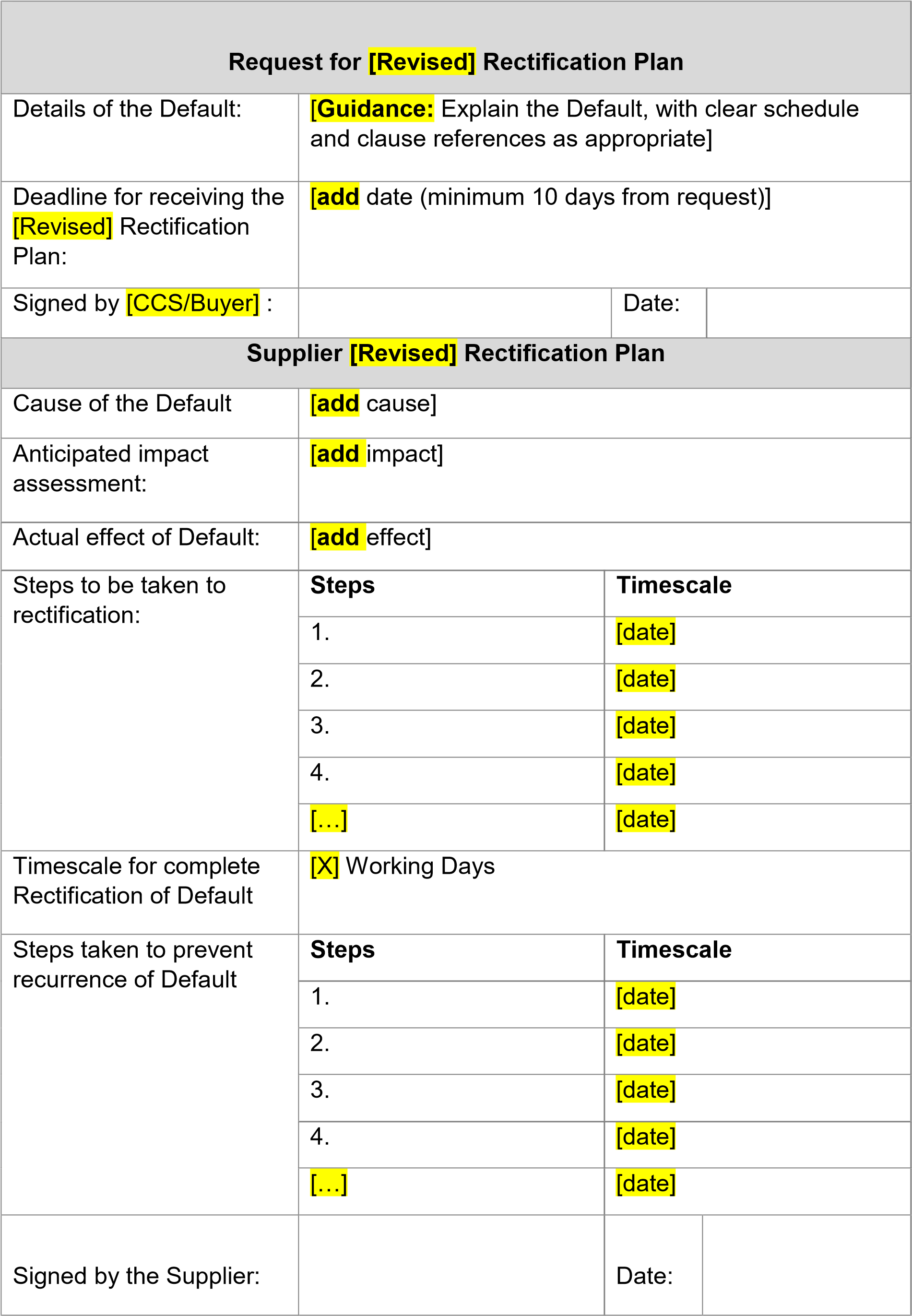
## ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following insurance cover from the DPS Start Date in accordance with this Schedule:
   1. professional indemnity insurance with cover for a single event or a series of related events and in the aggregate of not less than one million pounds (£1,000,000);
   2. public liability insurance with cover for a single event or a series of related events and in the aggregate of not less than one million pounds (£1,000,000); and
   3. employers’ liability insurance with cover for a single event or a series of related events and in the aggregate of not less than five million pounds (£5,000,000).

**Joint Schedule 10 (Rectification Plan)**

Crown Copyright2021

**Joint Schedule 10 (Rectification Plan)**



Project Version:v1.0 2 **Joint Schedule 10 (Rectification Plan)**

Crown Copyright2021

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Review of Rectification Plan** | | | | | | [CCS/Buyer] | |  | | |
|  | |
| Outcome of review | | |  | [Plan Accepted] [Plan Rejected] [Revised Plan | | | | | |  |
| Requested] | | | | | |
| Reasons for Rejection (if applicable) | | |  | [**add** | reasons] | | | | | |
|  |
| Signed by | [CCS/Buyer] |  |  | | | | Date: | |  | |
|  |

Project Version:v1.0 2

**Joint Schedule 11 (Processing Data)**

## Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

**“Processor** all directors, officers, employees, agents, consultants and

**Personnel”** suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

## Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection

Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) “Controller” in respect of the other Party who is “Processor”; (b) “Processor” in respect of the other Party who is “Controller”;

1. “Joint Controller” with the other Party;
2. “Independent Controller” of the Personal Data where the other Party is also

“Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

## Where one Party is Controller and the other Party its Processor

1. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.
2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
4. a systematic description of the envisaged Processing and the purpose of the Processing;
5. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
6. an assessment of the risks to the rights and freedoms of Data Subjects; and
7. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

1. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
2. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
   1. nature of the data to be protected;
   2. harm that might result from a Personal Data Breach;
   3. state of technological development; and
   4. cost of implementing any measures; (c) ensure that :
   5. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
   6. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
      1. are aware of and comply with the Processor’s duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
      2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
      3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
      4. have undergone adequate training in the use, care, protection and handling of Personal Data;
3. not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
   1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with

UK GDPR Article 46 or LED Article 37) as determined by the Controller;

* 1. the Data Subject has enforceable rights and effective legal remedies;
  2. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  3. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

1. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

1. receives a Data Subject Access Request (or purported Data Subject Access Request);
2. receives a request to rectify, block or erase any Personal Data;
3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
6. becomes aware of a Personal Data Breach.
7. The Processor’s obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
9. the Controller with full details and copies of the complaint, communication or request;
10. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
11. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
12. assistance as requested by the Controller following any Personal Data Breach; and/or
13. assistance as requested by the Controller with respect to any request from the

Information Commissioner’s Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

1. the Controller determines that the Processing is not occasional;
2. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
4. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
5. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
6. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
7. notify the Controller in writing of the intended Subprocessor and Processing;
8. obtain the written consent of the Controller;
9. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
10. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
11. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
12. The Relevant Authority may, at any time on not less than thirty (30) Working Days’ notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
13. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Relevant Authority may on not less than thirty (30) Working Days’ notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

## Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

## Independent Controllers of Personal Data

1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
5. The Parties shall only provide Personal Data to each other:
6. to the extent necessary to perform their respective obligations under the Contract;
7. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
8. where it has recorded it in Annex 1 *(Processing Personal Data).*
9. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent

Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

1. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
2. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **(“Request Recipient”)**:
3. the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
4. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
   1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
   2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
2. implement any measures necessary to restore the security of any compromised Personal Data;
3. work with the other Party to make any required notifications to the Information

Commissioner’s Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

1. not do anything which may damage the reputation of the other Party or that

Party's relationship with the relevant Data Subjects, save as required by Law.

1. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*
2. Personal Data shall not be retained or processed for longer than is necessary to perform each Party’s respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.
3. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 27 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority’s Data Protection Officer are: Tracey Kerr tracey.kerr@cabinetoffice.gov.uk

1.2 The contact details of the Supplier’s Data Protection Officer are: Ian Mafuta ian@constructeducation.com

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of  Controller for each  Category of  Personal Data | **The Relevant Authority is Controller and the Supplier is**  **Processor**  The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:   * *Name* * *Email* * *Organisation*     *For individuals booking events or requesting newsletters*   * *Name* * *Email*     *For individuals viewing webinars*   * *Web activity* * *Cookie IDs* * *IP addresses*     *For website users*   * *training and programme feedback* * *evaluation and/or user research purposes*     *For individuals answering surveys* |
| Duration of the Processing | *06/09/2024 – 06/09/2028* |
| Nature and purposes of the  Processing | Learner enrolment and processing, Learner experience improvement, website traffic analysis |
| Type of Personal Data | Name, Email, Organisation, IP Address, Cookie ID |
| Categories of Data Subject | Learner Data – Name, Email, Role, Organisation, Website Activity Data, Learner Feedback. |
| Plan for return and destruction of the data once the Processing is complete UNLESS  requirement under  Union or Member State law to preserve that type of data | Data will be retained for 4 years from commencement of the contract. Handling of the data will be inline with the DPIA |

## Annex 2 - Joint Controller Agreement – NOT USED 1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake

to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

1. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
2. shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
3. is solely responsible for the Parties’ compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
4. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
5. shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier’s/Relevant Authority’s] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

## 2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

1. report to the other Party every [x] months on:
   1. the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
   2. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
   3. any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party’s obligations under applicable Data Protection Legislation;
   4. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
   5. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

1. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
2. provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
3. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
4. request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
5. ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
6. take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
   1. are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
   2. are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
   3. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
7. ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
8. nature of the data to be protected;
   1. harm that might result from a Personal Data Breach;
   2. state of technological development; and
   3. cost of implementing any measures;
9. ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
10. ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

## 3. Data Protection Breach

3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

1. sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
2. all reasonable assistance, including:
   * 1. co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
     2. co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
     3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
     4. providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party’s own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

1. the nature of the Personal Data Breach;
2. the nature of Personal Data affected;
3. the categories and number of Data Subjects concerned;
4. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
5. measures taken or proposed to be taken to address the Personal Data Breach; and
6. describe the likely consequences of the Personal Data Breach.

## 4. Audit

4.1 The Supplier shall permit:

1. the Relevant Authority, or a third-party auditor acting under the Relevant

Authority’s direction, to conduct, at the Relevant Authority’s cost, data privacy and security audits, assessments and inspections concerning the Supplier’s data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

1. the Relevant Authority, or a third-party auditor acting under the Relevant Authority’s direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier’s compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

## 5. Impact Assessments

5.1 The Parties shall:

1. provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

1. maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

## 6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days’ notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

## 7. Liabilities for Data Protection Breach

**[Guidance:** This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

1. if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
2. if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
3. if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).
   1. If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“Court”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
   2. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):
4. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
5. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
6. if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

## 8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

## 9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

1. carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
2. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

## 10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

**Joint Schedule 12 (Supply Chain Visibility)**

## 1. Definitions

1.1In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

**"Contracts Finder"** the Government’s publishing portal for public sector procurement opportunities;

**"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;

**“Supply Chain Information** the document at Annex 1 of this Schedule

## Report Template” 12; and

**"VCSE"** a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

## 2. Visibility of Sub-Contract Opportunities in the Supply Chain

2.1 The Supplier shall:

2.1.1 subject to Paragraph 2.3, advertise on Contracts Finder all Sub-Contract opportunities arising from or in connection with the provision of the Deliverables above a minimum threshold of £25,000 that arise during the Contract Period;

2.1.2 within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contract Finder with details of the successful Subcontractor;

2.1.3 monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period;

2.1.4 provide reports on the information at Paragraph 2.1.3 to the Relevant

Authority in the format and frequency as reasonably specified by the Relevant Authority; and

2.1.5 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

2.2 Each advert referred to at Paragraph 2.1.1 of this Schedule 12 shall provide a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

2.3 The obligation on the Supplier set out at Paragraph 2.1 shall only apply in respect of Sub-Contract opportunities arising after the Effective Date.

2.4 Notwithstanding Paragraph 2.1, the Authority may by giving its prior Approval, agree that a Sub-Contract opportunity is not required to be advertised by the Supplier on Contracts Finder.

## 3. Visibility of Supply Chain Spend

3.1 In addition to any other management information requirements set out in the Contract, the Supplier agrees and acknowledges that it shall, at no charge, provide timely, full, accurate and complete SME management information reports (the “SME Management Information Reports”) to the Relevant Authority which incorporates the data described in the Supply Chain Information Report Template which is:

1. the total contract revenue received directly on the Contract;
2. the total value of sub-contracted revenues under the Contract

(including revenues for non-SMEs/non-VCSEs); and

1. the total value of sub-contracted revenues to SMEs and VCSEs.

* 1. The SME Management Information Reports shall be provided by the Supplier in the correct format as required by the Supply Chain Information Report Template and any guidance issued by the Relevant Authority from time to time. The Supplier agrees that it shall use the Supply Chain Information Report Template to provide the information detailed at Paragraph 3.1(a) –(c) and acknowledges that the template may be changed from time to time (including the data required and/or format) by the Relevant Authority issuing a replacement version. The Relevant

Authority agrees to give at least thirty (30) days’ notice in writing of any such change and shall specify the date from which it must be used.

* 1. The Supplier further agrees and acknowledges that it may not make any amendment to the Supply Chain Information Report Template without the prior Approval of the Authority.

**Annex 1**

**Supply Chain Information Report template**

