

G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

G-Cloud 14 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	15
Schedule 1: Services	36
Schedule 2: Call-Off Contract charges	37
Schedule 3: Collaboration agreement	39
Schedule 4: Alternative clauses	40
Schedule 5: Guarantee	45
Schedule 6: Glossary and interpretations	46
Schedule 7: UK GDPR Information	63
Annex 1: Processing Personal Data	63
Annex 2: Joint Controller Agreement	65
Schedule 8: Corporate Resolution Planning	66
Schedule 9 : Variation Form	81
Schedule 10 : Operational Requirements	83
Schedule 11 : Departmental Security Standards	88
Appendix 1 : G-Cloud 14 Service Definition	98
Appendix 2 : G-Cloud 14 Service Pricing	

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	614452403468448
Call-Off Contract reference	Con_26713
Call-Off Contract title	Course Directory Support Services
Call-Off Contract description	<p>Educational establishments use National Careers Service Course Directory "provider portal" to update details of all courses they offer. This allows the public to search for suitable courses using third party websites as all records are held within our central data warehouse as open data which third parties can freely consume using an API.</p> <p>The contract includes:</p> <ul style="list-style-type: none">• The Operational Service <p>The scope of this service is described below under Buyer Contractual Details in this Order Form</p>
Start date	01/03/2025
Expiry date	31/08/2026
Call-Off Contract value	£ [REDACTED] exc. VAT

Charging method	Monthly invoice in arrears for the Services delivered. The Supplier shall issue electronic invoices based on payment profiles at Schedule 2. The charging model is fixed price for each work package commissioned unless otherwise agreed between the Parties as part of a Request for Quote (RFQ).
Purchase order number	To be provided by the Buyer to the Supplier within 14 days from signing this Order Form.

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	The Secretary of State for the Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
-----------------------	--

To the Supplier	Tribal Education Limited St Mary's Court 55 St Mary's Road Sheffield S2 4AN Company number: 04163300
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: [REDACTED]
Name: [REDACTED]
Email: [REDACTED]
Phone: [REDACTED]

For the Supplier:

Title: [REDACTED]
Name: [REDACTED] [REDACTED]
Email: [REDACTED]
Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01/03/25 and is valid for 18 months .
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p> <p>In the event that Buyer funding is withdrawn for FY 26/27, the Buyer may terminate the Call-Off Contract without cause or penalty in accordance with the notice period outlined above.</p>
Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 30 days written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none">● Lot 2: Cloud software
--------------------	---

**G-Cloud Services
required**

The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 10 and outlined below:

The Operational Services including:

- Identity and authentication services
- Proactive data quality monitoring
- Proactive assistance to help providers improve their data in line with agreed metrics/measures
- Onboarding providers, including apprenticeship trainers, and supporting the standardisation of their data
- Supporting DfE
- User support
- In-system support for audit information

The supplier shall provide a data quality management service supporting the DfE cloud hosted Course Directory platform which also host or links providers courses and applications from their hosted platforms. Currently, there are 2,567 providers in total (on the hosted Course Directory Platform) with 110,000 courses.

The number may change (up and down) over the contract period.

In the event that the number of providers increases by more than 10% from the baseline figure of 2,567 given above, then the Buyer and the Supplier, acting in good faith, will seek to agree a mechanism to adjust the Charges accordingly.

In line with the above, the supplier will provide a suite of services which shall be considered more than just a helpdesk support including the following:

- Operational Support Helpdesk
- Data quality monitoring and assurance services (including reporting)
- Support to the Customer
- User support for the education and training providers who submit their course data and apprenticeship data

DfE do not mandate the supplier to use specific software or applications as part of their own management and delivery and the supplier will have access to the DfE systems to manager and deliver this application on behalf of DfE.

DfE use the Azure platform with the following applications:

Microsoft Azure:

- .NET Core

	<ul style="list-style-type: none"> • Functions v3 • SQL Server • Cosmos (To be deprecated) • Azure Cognitive Search • API Management • Application Insights <p>The supplier will work together with the buyer (DfE) to ensure compliance with relevant standards, knowhow and compatibility of any support software to be used to support effective delivery. The detailed service specification is attached at Schedule 10.</p>
Additional Services	<p>Any additional services as listed in the Suppliers Service Description. Any additional services required will be included by way of formal Variation and Request for Quote (RfQ) from the Supplier.</p> <p>The Buyer reserves the option to procure additional services in line with the Buyer's requirements. This may include additional Professional Services provided on a fixed price or time and materials (T&M) basis and will be agreed between the Buyer and the Supplier following completion of the Request for Quote for Additional Services Template embedded as "RfQ" in the 'Supplemental requirements' section of this Call-Off Contract.</p>
Location	<p>The Services will be delivered to remote providers throughout England, but DfE support will be provided to offices in Sheffield and Coventry.</p>
Quality Standards	<p>The Supplier will carry out the services with reasonable care and skill. All services supplied shall exceed, or be fit for the particular purpose, for which they are supplied with reference to the Customer's requirements - in line with quality standards detailed in the Supplier's offering on G-Cloud 14.</p> <p>The minimum quality standards required for this Call-Off Contract are:</p> <ul style="list-style-type: none"> • ISO/IEC 27001 – information security management • ISO 9001 – quality management
Technical Standards:	<p>The Supplier will carry out the services with reasonable care and skill. All services supplied shall exceed, or be fit for any specified purpose for which they are supplied with reference to the Customer's requirements, as specified in Schedule 10, in line with technical standards detailed in</p>

	the Supplier's offering on G-Cloud 14.
Service level agreement:	<p>The minimum service level and availability criteria required for this Call-Off Contract are:</p> <ul style="list-style-type: none"> • Helpline availability 09.00-17.00 GMT/BST Monday to Friday excluding bank holidays, within the jurisdiction • 90% Calls/ messages/ mails acknowledged within 0.5 support hours • 100% Calls/ messages/ mails acknowledged within 1.0 support hours • 95% Calls/ messages/ mails rectified within 1 working day (if rectification does not require 3rd party input) • 90% incidents needing to be forwarded to DfE Service Now done so within 0.5 service hours • 100% incidents needing to be forwarded to DfE Service Now done so within 1.0 service hours • 90% of data quality incidents have initial contact and scheduled follow-up within 1 working day, subject to provider user availability • 100% of data quality incidents have initial contact and scheduled follow-up within 2 working days, subject to provider user availability.
Onboarding	<p>The onboarding plan for this Call-Off Contract is:</p> <p>The Supplier will, working in conjunction with the Customer's team:</p> <ul style="list-style-type: none"> • Propose and agree provider data quality measures • Produce a provider communications plan • Produce updated provider communication collateral.
Offboarding	<p>The offboarding plan for this Call-Off Contract is through an updated exit plan that must be delivered within 2 months of the Operational Service going live and is then reviewed on an annual basis thereafter. The final monthly payment shall be made once the Off-boarding plan has been executed to the Client's satisfaction and the Client shall confirm its acceptance no later than 14 days from the executed Off-boarding plan.</p>
Collaboration agreement	<p>No Collaboration agreement is anticipated. Interfaces between the Parties will be managed jointly.</p>

<p>Limit on Parties' liability</p>	<p>Defaults by either party resulting in direct loss or damage to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £1,000,000 per year.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
<p>Buyer's responsibilities</p>	<p>The Buyer is responsible for:</p> <p>During the Operational Service:</p> <ul style="list-style-type: none"> • Providing access to provider data • Development / deployment of in-system reports to enable data quality assurance and monitoring • Attendance at quarterly account review meetings • Management of calls escalated to the Agency for resolution • Provision of guidance on relevant policy as required • Provision of reports or reporting capability on provider data • Provision of timely information on providers needing to be on-boarded to the service • Ad hoc confirmation of whether a provider has a contract for Agency funded provision • Updates on changes to the system or data specifications prior to the updates being made

Buyer's equipment	Not applicable.
--------------------------	-----------------

Supplier's information

Subcontractors or partners	Not applicable.
-----------------------------------	-----------------

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is electronic payment via BACS.
Payment profile	The payment profile for this Call-Off Contract is monthly in arrears in accordance with Schedule 2, for the Operational Service.
Invoice details	<p>The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.</p> <p>The Supplier shall work with the Buyer to minimise the impact on the public purse for T&S associated with the operation of this contract. If</p>

	<p>expenditure on T&S is identified as being necessary, T&S will be paid at the level commensurate with the DfE rate in place at the time the expenditure is incurred.</p>
<p>Who and where to send invoices to</p>	<p>Invoices to be sent electronically to AccountsPayable.OCR@education.gov.uk. All invoices must include a valid Purchase Order number.</p>
<p>Invoice information required</p>	<p>All invoices must include:</p> <ul style="list-style-type: none"> • the date of the invoice; • a unique invoice number; • Supplier's full name and address; • a valid purchase order reference • quotes a valid Purchase Order number (prefix – CORE-PO-); • the charging period; • a detailed line level breakdown of the appropriate Charges including Services provided; • Charges in Great British Pound Sterling (£); and, • Payable UK VAT. <p>All invoices must also be in an un-editable format (such as PDF), and be in accordance with the Charges agreed with the Buyer, as outlined within this Call-Off Contract.</p> <p>Invoices without a valid purchase order are now rejected by the Buyers e-invoicing solution. The Buyer no longer accepts paper invoices.</p>
<p>Invoice frequency</p>	<p>Invoice will be sent to the Buyer monthly in arrears.</p>
<p>Call-Off Contract value</p>	<p>The total value of this Call-Off Contract is £ XXXXXXXXXX exc. VAT.</p> <p>Both Parties acknowledge that the above figure is a maximum Contract Value incorporating contingency. Both Parties shall work together on an ongoing basis during the term of the Contract to define the actual Resources required by the Buyer from the Supplier through the planning and definition of separate RfQs which shall become part</p>

	of this Call-Off Contract. The contract does not guarantee of the full level of spend against the contract value
Call-Off Contract charges	<p>The breakdown of the Charges is as set out at Schedule 2.</p> <p>Unless otherwise agreed by the Parties, all current and future charges will not exceed the applicable Call-Off Contract charges (in accordance with the Supplier's Digital Marketplace pricing document) during the term of the Call-Off Contract.</p>

Additional Buyer terms

Performance of the Service	As specified in Schedule 10 - The Course Directory Operational Service Requirements
Guarantee	Not applicable.
Warranties, representations	As per the incorporated Framework Agreement clause 2.3.

Supplemental requirements in addition to the Call-Off terms	The DfE Security Policy attached should be adhered to, as laid out in Schedule 11.
Alternative clauses	Not applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>In the event of conflict, the order of precedence shall be as follows:</p> <ul style="list-style-type: none"> • G-Cloud 14 Framework Agreement • G-Cloud 14 Order Form • G-Cloud 14 Call-Off Contract • Buyer's Supplemental Security Clauses • Supplier Terms and Conditions
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1
Intellectual Property	The licence granted under clause 11.2 shall only apply to any Project Specific IPRs and Background IPRs which form part of the tangible outputs of the G-Cloud Services delivered to the Buyer. Any rights not expressly granted to the Buyer are reserved to the Supplier
Social Value	<p>The Supplier has committed to achievement of the following Social Value KPI:</p> <p>Number of full-time equivalent (FTE) employment opportunities created under the contract, by UK region.</p> <p>Service Level Target: 1 employment opportunity</p>
Performance Indicators	<p>Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.</p> <p>[Note required Performance Indicators needed from the Supplier for future publication or otherwise]</p>

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.







1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.

2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	Buyer
Name		
Title		
Signature		
Date	13/03/25	13/03/25

Buyer Benefits

For each Call-Off Contract please complete a buyer benefits record, by following this link:

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 36 months

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)

- 26 (Equality and diversity)
- 28 (Data protection)
- 30 (Insurance)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

- 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
- 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
- (b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
- (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security - Classification policy:
<https://www.gov.uk/government/publications/government-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.npsa.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets: <https://www.npsa.gov.uk/sensitive-information-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:
<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:
<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:

<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 Any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more

than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited;
and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who is not a Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately

disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- 29.2.1 the activities they perform
- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work
- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements
- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29.2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will cooperate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

- 29.6.1 its failure to comply with the provisions of this clause

- 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.3 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.4 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 if it isn't a material change to the Framework Agreement or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request using the template in Schedule 9. This includes any changes in the Supplier's supply chain.

32.3 If either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days' notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

The Buyer Requirements shall be as defined under G-Cloud Services required in the Buyer Contractual details Section of the Order Form.

In providing the resource to deliver all of the above the supplier shall:

- use its own initiative as to the manner in which services are to be delivered
- not be supervised, directed or controlled regarding how the services are delivered
- use its own equipment where security requirements permit
- be expected to provide the services on such hours/days as required to meet any deadlines, as agreed between the supplier and the buyer
- provide the necessary resources to support the Services which shall include one or more specialists
- link the payment to outputs and deliverables

The buyer is willing to accept substitute personnel with the relevant skills and expertise. The Supplier is responsible for ensuring the achievement of Deliverables is not impacted and as per the Supplier's Service Definition, the Supplier agrees to undertake this as their own expense.

The Supplier Services to be provided under this Call-Off Contract shall be as set out in its G-Cloud 14 Service Offerings as attached at Schedule 9.

Schedule 2: Call-Off Contract Charges

For each individual Service, the applicable Call-Off Contract charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will be as below, as specified in Tribal's G-Cloud Pricing document attached at Schedule 10.

Table 3 – Fees Service	Cost for initial 18-month contract period 2025/2026	Cost for 12-month optional extension	Total Cost
Core contract: User support and data quality management of course providers**	£ [REDACTED]	£ [REDACTED]	£ [REDACTED]
Apprenticeships: Standardisation up to 200 new APAR applicants onboarded and Quality Assured*	£ [REDACTED]	£ [REDACTED]	£ [REDACTED]
Total	£ [REDACTED]	£ [REDACTED]	£ [REDACTED]

**To a maximum of 3,200 onboarded providers and 180,000 live courses. For reference, there are currently 2,567 providers and 110,000 courses. This increase comfortably allows for onboarding of new provider types during the contract period.

*Where the number of new applicants to APAR onboarded and Quality Assured exceeds 200 charges are as shown in table 4 below. This includes standardisation of a 5% sample of the additional providers. For reference, there were fewer than 70 new APAR providers onboarded.

Table 4 – Fees p.a. for additional new APAR applicants over 200 Provider applicant numbers over the 200 p.a.	Cost p.a.
1-50	£ [REDACTED]
51-100	£ [REDACTED]
101-200	£ [REDACTED]

Charges

1. The Parties agree that any assumptions, representations, risks and contingencies stated in any RfQ will apply in relation to the Charges calculated for that RfQ.
2. Any work for which a proportion fails to meet the Acceptance Criteria in a specified period will not be accepted by the Buyer and will be completed at the Supplier's expense. The Charges applied to that proportion of work will be excluded from the total Charges due for that period. Those Charges so excluded may only be charged once the quality and standard of the work for that period has been accepted by the Buyer
3. Working periods shall be Monday to Friday (excluding national holidays) unless agreed in advance with days based upon a Professional working day.
4. Travel and Subsistence shall be payable (with advance agreement) in line with DfE T&S policy for work delivered at alternative sites.

5. In agreeing an RfQ, the Supplier and Buyer may agree to a fixed price for stated deliverables. Fixed charges will be based upon the Supplier's calculation of resource costs and the estimated duration.

6. The Buyer will not pay more than the Day Rates for the SFIA grade required if a higher graded resource is used by the Supplier at its own choice.

Schedule 3: Collaboration agreement

Not applicable.

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Buyer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Buyer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996

- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use its best endeavours to ensure that in its employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract it promotes equality of treatment and opportunity between:

- a. persons of different religious beliefs or political opinions
- b. men and women or married and unmarried persons
- c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- f. persons of different ages
- g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Buyer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- a. the issue of written instructions to staff and other relevant persons
- b. the appointment or designation of a senior manager with responsibility for equal opportunities
- c. training of all staff and other relevant persons in equal opportunities and harassment matters
- d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Buyer as soon as possible in the event of:

- A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Term by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Buyer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Buyer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Buyer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Buyer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Buyer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Buyer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Buyer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Buyer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Buyer premises, the Supplier will comply with any health and safety measures implemented by the Buyer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Buyer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Buyer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Buyer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Buyer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).

2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

Not applicable.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none">• owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes• created by the Party independently of this Call-Off Contract, or <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form, set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').

Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(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 Subject	Takes the meaning given in the UK GDPR

Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.

Employment Status Indicator test tool or ESI tool	<p>The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax</p>
Expiry Date	<p>The expiry date of this Call-Off Contract in the Order Form.</p>
Financial Metrics	<p>The following financial and accounting measures:</p> <ul style="list-style-type: none"> • Dun and Bradstreet score of 50 • Operating Profit Margin of 2% • Net Worth of 0 • Quick Ratio of 0.7
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into

	<ul style="list-style-type: none"> any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.14 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.

Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that 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 in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Supplier Trigger Event
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <p>(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</p> <p>(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</p> <ul style="list-style-type: none"> • (c) all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR claim	As set out in clause 11.5.

IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the 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, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of

	VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.

Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see

	https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
-----------------------	---

Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	<p>An assessment of the impact of a variation request by the Buyer completed in good faith, including:</p> <ul style="list-style-type: none"> a) details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract; b) details of the cost of implementing the proposed variation; c) details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the variation; and <p>such other information as the Buyer may reasonably request in (or in response to) the variation request;</p>
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.

Year	A contract year.
-------------	------------------

Intentionally Blank

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended

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 Buyer at its absolute discretion.

- 1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] . Email – [REDACTED] .
- 1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] – Email - [REDACTED]
- 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 and Processor for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">• Any Personal Data which is Processed by the Supplier during:<ul style="list-style-type: none">○ The contracting and ordering process○ The delivery of associated support services; and,○ The delivery of general administrative services in respect to the Contract (e.g., billing, etc). <p>For clarity, the Supplier will make use of a CRM system for delivery of the service and for reporting, but the Supplier will not be acting as Data Controller.</p>
Duration of the Processing	<p>01/03/25 – 31/08/26</p> <p>And for up to 1 x 12 month extension period to 30/08/27 that may be agreed under the Terms of this Agreement.</p>

Nature and purposes of the Processing	<p>The nature of the Processing includes 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 data (whether or not by automated means).</p> <p>The purpose of the Processing is delivery of the Publish to the Course Directory Operational Service including user support helpdesk, reporting, technical incident resolution, complaints management and providing advice and support to the customer.</p>
Type of Personal Data	<p>Name</p> <p>Job title</p> <p>Contact details</p> <p>Employing organisation</p>
Categories of Data Subject	<p>Users of Publish to the Course Directory</p> <p>Customer staff</p> <p>Buyer staff</p>
International transfers and legal gateway	<p>All Personal Data must be Processed/Stored within the United Kingdom.</p>
Plan for return and destruction of the data once the Processing is complete	<p>The supplier will destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed.</p>

Annex 2 - Joint Controller Agreement

Not applicable.

Schedule 8 (Corporate Resolution Planning)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Annual Revenue"	<p>means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:</p> <p>figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and</p> <p>where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;</p>
"Appropriate Authority" or "Appropriate Authorities"	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;

“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Cabinet Office Markets and Suppliers Team"	means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“Control”	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Corporate Change Event”	means: (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;

	<p>(c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;</p> <p>(d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;</p> <p>(e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;</p> <p>(f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;</p> <p>(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;</p> <p>(h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;</p> <p>(i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or</p> <p>(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;</p>
"Corporate Change Event Grace Period"	means a grace period agreed to by the Appropriate Authority for providing CRP

	Information and/or updates to Business Continuity Plan after a Corporate Change Event;
"Corporate Resolvability Assessment (Structural Review)"	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;
"Critical National Infrastructure" or "CNI"	<p>means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>significant impact on the national security, national defence, or the functioning of the UK;</p>
"Critical Service Contract"	means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;
"CRP Information"	means the corporate resolution planning information, together, the:

	<p>(a) Exposure Information (Contracts List);</p> <p>(b) Corporate Resolvability Assessment (Structural Review); and</p> <p>(c) Financial Information and Commentary</p>
“Dependent Parent Undertaking”	<p>means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;</p>
“FDE Group” “Financial Distress Event”	<p>means the Supplier</p> <p>the credit rating of an FDE Group entity dropping below the applicable Financial Metric;</p> <p>an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;</p> <p>there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;</p> <p>an FDE Group entity committing a material breach of covenant to its lenders;</p> <p>a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;</p> <p>any of the following:</p> <p>commencement of any litigation against an FDE Group entity with respect to financial indebtedness</p>

	<p>greater than £5m or obligations under a service contract with a total contract value greater than £5m;</p> <p>non-payment by an FDE Group entity of any financial indebtedness;</p> <p>any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;</p> <p>the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or</p> <p>the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;</p> <p>in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and</p> <p>any two of the Financial Metrics for the Supplier not being met at the same time.</p>
“Parent Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Public Sector Dependent Supplier”	means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Subsidiary Undertaking”	

	has the meaning set out in section 1162 of the Companies Act 2006;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and
“UK Public Sector / CNI Contract Information”	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;

2. Service Status and Supplier Status

2.1 This Call-Off Contract is not a Critical Service Contract.

2.2 The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is resolution.planning@cabinetoffice.gov.uk.

2.3 The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer's rights under this Schedule.

3. Provision of Corporate Resolution Planning Information

3.1 Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.

3.2 Subject to Paragraphs 3.6, 3.10 and 3.11:

3.2.1 where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and

3.2.2 except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.

3.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

3.3.1 is full, comprehensive, accurate and up to date;

3.3.2 is split into three parts:

- (a) Exposure Information (Contracts List);
- (b) Corporate Resolvability Assessment (Structural Review);
- (c) Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

3.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

3.3.4 provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and

3.3.5 complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

3.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

3.5 If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

3.5.1 the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

3.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

3.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

3.7 An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

3.7.1 the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and

3.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.

3.8 If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

3.8.1 within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11) unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;

3.8.2 within 30 days of a Corporate Change Event unless

(a) the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the

nature of the Corporate Change Event and the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

(b) not required pursuant to Paragraph 3.10;

3.8.3 within 30 days of the date that:

(a) the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or

(b) none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

3.8.4 in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

(a) updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or

(b) not required pursuant to Paragraph 3.10.

3.9 Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

3.10 Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

3.10.1 Aa3 or better from Moody's;

3.10.2 AA- or better from Standard and Poors;

3.10.3 AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

3.11 Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant

information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

4. Termination Rights

4.1 The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

4.1.1 the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

4.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

5. Confidentiality and usage of CRP Information

5.1 The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.

5.2 Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.

5.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

5.4 Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

5.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;

5.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:

(a) summarising the information;

(b) grouping the information;

(c) anonymising the information; and

(d) presenting the information in general terms

5.5 The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP

Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST

1 The Supplier shall:

1.1 provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:

(a) are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;

(b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or

(c) involve or could reasonably be considered to involve CNI;

1.2 provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

1. The Supplier shall:

1.1 provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;

1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and

1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information AND COMMENTARY

1 The Supplier shall:

1.1 provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and

1.2 ensure that the information is presented in a simple, effective and easily understood manner.

2 For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	[insert name of Buyer] ("the Buyer") And [insert name of Supplier] ("the Supplier")	
Contract name:	[insert name of contract to be changed] ("the Contract")	
Contract reference number:	[insert contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete] as applicable: Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
A Variation Impact Assessment shall be provided within:	[insert number] 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: <ul style="list-style-type: none"> [Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause] 	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]

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 Buyer

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.

Signed by an authorised signatory for and on behalf of the Buyer

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

Schedule 10 The Course Directory Operational Service Requirements

Introduction

The Department for Education (the DfE) is looking to procure the services to manage its Course Directory Service.

The Course Directory service is hosted and supported from within the DfE. The operational services in respect of data quality management and user support will remain outsourced and the requirements are described in this document.

Strategic Context

Since its launch in April 2010, the remit of the Course Directory has extended considerably. The Agency is now able to offer a more comprehensive search tool for all publicly funded and accredited provision. We are now actively engaged with nearly 5000 schools, 6th form colleges, FE colleges and training providers.

In December 2017 the government published a careers strategy that said:

- the National Careers Service will be the sole provider of careers information, advice and guidance to young people and adults. This will be provided via a new website, alongside a range of tools that individuals, advisors and schools can use.
- an improved course directory will clearly explain routes to a wide range of vocational and academic learning opportunities, including apprenticeships, degrees and basic skills courses.

In January 2021, the government published the skills for jobs white paper which included the following two objectives:

Putting employers at the heart of post 16 skills,

Advanced higher and technical skills

People need access to the information, advice and guidance that will help them make choices about education, training and their careers.

In support of these aims, the Agency has made this full range of provision not only available through the National Careers Service online channel, but also freely available to any third parties through download from www.data.gov.uk meaning they can make innovative use of the data and present it in ways more meaningful to their audience.

The Course Directory also collects information about apprenticeship training and publishes information on 'Find apprenticeship training' in the apprenticeship service. This enables employers to search for apprenticeship standards delivered by providers in a location of their choice.

The successful bidder will recognise the increasing strategic importance of the Course Directory and will be committed to ensuring that the data is of the highest quality possible. They will do so by working with providers to ensure widespread best practice in data submission and management.

Overview of the requirement

The service requirement comprises:

- Data quality monitoring and assurance services (including reporting)
- Support to the Department

- User support for the education and training providers who submit their course data and apprenticeship data

Currently the number of providers registered on this service is 2,567 (based on February 2025 data). We expect some increase in provider numbers (at least 10%) to be covered by the service price, but there are refresh processes whereby provider contracts are retendered and so some providers may exit whilst others may need to be on-boarded, so some fluctuations in numbers need to be expected.

It should be pointed out that more providers are registered with the course directory than use it, especially for private work based (apprenticeships) providers, who may join the register of Apprenticeship training providers, but not then be commissioned to provide training by employers.

Data Quality management

A data quality management service which will include proactive engagement with providers in support of the Department's commitment to collect and make available comprehensive and accurate information.

The Course Directory provides public facing data and it is important that the quality of data is of the highest standard

The contractor will work with the Department to develop appropriate data quality metrics and propose dashboards to enable the contractor to monitor provider submissions against the agreed metrics. The metrics should cover timeliness of data (updates and retiring out of date courses); comprehensiveness of data (in comparison to other official sources) and the accuracy of the data.

The contractor will carry out ongoing quality checks on apprenticeship data on a percentage of providers and their data. This will be based on a sliding scale depending on the number of apprenticeship entries a provider has. In addition, the contractor will report on the timeliness of data based on agreed KPIs. The contractor will develop a plan for improving data quality and associated reporting and will inform and support the testing and development of appropriate reports and dashboards by the Department. The contractor will engage with providers to make sure that data quality reporting is relevant to providers and meaningful in terms of quality for end users.

The contractor will provide detailed monthly performance summaries of provider data (or lack of) based on the data quality reports and dashboards, but also to include engagement with providers to enable effective management of the quality of the Course Directory as a whole. Business and Service Reporting¹ – weekly (scheduled day agreed with the business with exception of bank holidays) and monthly (to be delivered no later than the close of working hours on the fifth working day of the month following that to which the report relates). The format and frequency of future reporting will be agreed with the Department during the transition period.

It is a condition of the Department for Education's funding that FE learning providers upload their information to the Course Directory at least every 3 months and schools upload their information every 12 months, but the expectation is that FE providers will update as often as

¹ Due to the ongoing development of the service, reporting requirements are subject to change

necessary in order to maintain an accurate and comprehensive set of course information². For apprenticeships, providers are required to record and maintain up-to-date information about the apprenticeship training it offers in the Publish to the Course Directory Provider Portal.

For courses the current provider data and venue data requirements for the various data fields are set out in Publish to the Course Directory.

The provider portal is designed to minimise the burden of data collection and to be easier to use for validating and submitting data. This means that the data quality challenge will change. This also means that the metrics for data quality will have to evolve and the contractor is expected to provide some expertise in evolving how data quality is measured.

For apprenticeships there are guidance documents on how to submit data on the Publish to the Course Directory Provider Portal at:

<https://www.gov.uk/government/publications/find-apprenticeship-training-how-to-submit-data>

Data supplied by providers will be quality checked against these documents.

The Provider Data Standards document identifies mandatory and desirable data needed by the Course Directory and recommends standards for those fields

The current scope for the data collection to the Course Directory is:

- All Adult (19+) courses funded by the DfE
- 16-18 provision delivered by providers with DfE contracts or DfE school contracts
- 16-19 courses funded by the DfE
- apprenticeships standards and apprenticeship frameworks funded by the DfE
- Higher Education Courses, to include all full-time and part-time undergraduate and postgraduate degrees
- Full-cost provision delivered by providers with DfE contracts

The contractor is responsible for assuring the accuracy of the data capture prior to publication, for example out of date courses and ensuring providers have correct contact details

Support to the Department

Ad-hoc advice / consultation to the Department about provider issues

Contacting providers to resolve non-compliance issues, or complaints, advising and signposting providers.

Communicating to providers as and when requested by the Department or need arises.

One-off targeted calls to specific providers to understand barriers/ issues and to help improve the apprenticeship service

Weekly / regular calls with the Department (apprenticeship service team & FE service team) to update on progress, issues, reporting etc

User support services

A first line helpdesk and call logging tools to provide first point of contact for all end users of the service.

² The data collection remit is subject to change.

The helpline will be available during working hours by telephone and email 09.00-17.00, Monday to Friday, excluding bank holidays.

The contractor will offer support throughout the whole Course Directory process including error resolution, providing ad-hoc advice, support to new and existing users and continually providing any additional support if needed. This support has been pivotal in helping to raise the engagement between providers and the Course Directory, and is seen as a 'must have' if the data in the Course Directory of the future continues to be well populated with good data.

User support will include:

Support for logging and resolving incidents that prevent or constrain data collection or reporting processes.

The contractor will be responsible for building and maintaining relationships with learning providers in order to maintain data quality and integrity.

User support for setting up and managing accounts, including recovery

User support for on-boarding new providers and off-boarding providers who are exiting the service, with dedicated support for register of apprenticeship training providers (RoATP) and applicants to the portal. NB there is a online quality assurance process that needs to be undertaken for every new apprenticeship provider on RoATP.

Signposting alternative services when providers call about matters other than the course directory.

Supporting and maintaining alignment of provider accounts and account information to processes that refresh or modify provider's qualification to offer services, e.g. procurement cycles, intervention.

Managing provider communications to ensure that they understand the benefits of using the course directory and are constructively engaged in submitting course and apprenticeship and T Level data.

Communicating any outages or other maintenance issues to providers as provided by the Department.

Passing any application issues through to the Department for resolution.

Indirect user support needs to be provided in respect of writing/ updating guidance documents, newsletters, collating provider feedback and attending DfE events, including provider events to promote the service.

The contractor will need to support the introduction of other additional datasets for data enrichment purposes and ensure documentation and training material reflects the service changes, for example, T-levels and on-boarding

Call length varies from 5 to 45 minutes depending on the complexity of the query; skills of the user; availability/ ease of contacting the user. Call volumes currently vary according to the time of year, from 330 to 1100+ per month.

The contractor will ensure they have appropriate infrastructure and systems to support the service they provide.

The contractor will adhere to non-functional requirements (see Appendix 1).

Appendix 1 – Non-functional requirements

NFR	Description	90% Responses * within	100% Responses * within....	95% Rectified ** within	Support hours (SLA)
Support calls	Telephone calls, messages or emails are acknowledged and any further information needed to understand or resolve or schedule a resolution for a problem in accessing or using the service	0.5 support hour	1 support hours	1 working day (if rectification does not require third party input)	09:00 – 17:00 Mon – Friday Excluding United Kingdom Public Holidays
Incident reporting	Where a support call needs an incident to be reported through to ServiceNow for resolution by the Agency hosting or application team	0.5 support hour	1 support hours	Depends on scale of incident, but reports back to incident reported must be initially within 1 hour and then at least daily	09:00 – 17:00 Mon – Friday Excluding United Kingdom Public Holidays
Data quality problems	Where a data quality problem is highlighted that requires an engagement with a provider, e.g. training, documentation, advice or guidance, then the initial contact to discuss the need and schedule a follow-up if required	1 working day	2 working days	n/a	08:00 – 17:30 Mon – Friday Excluding United Kingdom Public Holidays
Response = time from when the user logs the call with the Service Desk to when the user is advised of the course of action and estimated time for fix.					
Rectified = time from when the user logs the call with the Service Desk to when the user is advised that the incident or request has been rectified.					

Schedule 11 Departmental Security Standards

1. Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

“BPSS” “Baseline Personnel Security Standard”	the Government’s HMG Baseline Personal Security Standard. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
“CCSC” “Certified Cyber Security Consultancy”	is the National Cyber Security Centre’s (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
“CCP” “Certified Professional”	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
“CPA” “Commercial Product Assurance”	is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
“Cyber Essentials” “Cyber Essentials Plus”	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the

	<p>scheme; the link below points to these providers:</p> <p>https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body</p>
<p>“Data” “Data Controller” “Data Protection Officer” “Data Processor” “Personal Data” “Personal Data requiring Sensitive Processing” “Data Subject”, “Process” and “Processing”</p>	<p>shall have the meanings given to those terms by the Data Protection Legislation.</p>
<p>"Buyer's Data" "Buyer's Information"</p>	<p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including:</p> <p>(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:</p> <p>(i) supplied to the Supplier by or on behalf of the Buyer; or</p> <p>(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or</p> <p>(b) any Personal Data for which the Buyer is the Data Controller;</p>
“Departmental Security Standards”	<p>the Buyer's security policy or any standards, procedures, process or specification for security that the Supplier is required to deliver.</p>
“Digital Marketplace / G-Cloud”	<p>the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.</p>
“End User Devices”	<p>the personal computer or consumer devices that store or process information.</p>

“Good Industry Standard” “Industry Good Standard”	the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“GSC” “GSCP”	the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
“HMG”	Her Majesty’s Government
“ICT”	Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	the National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk

“OFFICIAL” “OFFICIAL-SENSITIVE”	<p>the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP).</p> <p>the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.</p>
“RBAC” “Role Based Access Control”	<p>Role Based Access Control, a method of restricting a person’s or process’ access to information depending on the role or functions assigned to them.</p>
“Storage Area Network” “SAN”	<p>an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.</p>
“Secure Sanitisation”	<p>the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.</p> <p>NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</p> <p>The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction-0</p>
“Security and Information Risk Advisor” “CCP SIRA” “SIRA”	<p>the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</p>
“Senior Information Risk Owner” “SIRO”	<p>the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arm’s length</p>

	bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
“SPF” “HMG Security Policy Framework”	the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

2. Operative Provisions

2.1. The Supplier shall be aware of and comply the relevant [HMG security policy framework](#), [NCSC guidelines](#) and where applicable Departmental Security Standards which include but are not constrained to the following paragraphs.

2.2. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of [Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification](#) - [Action Note 09/14](#) dated 25 May 2016, or any subsequent updated document, are mandated, namely that “contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract”. The certification scope shall be relevant to the Services supplied to, or on behalf of, the Buyer.

2.3. Where paragraph 2.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the Services supplied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

2.4. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer’s Data being handled in the course of providing the Services and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the

HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).

2.5. Buyer's Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required in line with paragraph 2.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

2.6. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the Services, and that store or process Buyer's Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

2.7. The Supplier shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Buyer's Data. This policy should include appropriate segregation of duties and if applicable role-based access controls (RBAC). User credentials that give access to Buyer's Data or systems shall be considered to be sensitive data and must be protected accordingly.

2.8. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to:

- physical security controls;
- good industry standard policies and processes;
- malware protection;
- boundary access controls including firewalls, application gateways, etc;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- use of secure device configuration and builds;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
- any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
 - retained and protected from tampering for a minimum period of six months;
 - made available to the department on request.

2.9. The Supplier shall ensure that any Buyer's Data (including email) transmitted over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.

2.10. The Supplier shall ensure that any Buyer's Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer except where the Buyer has given its prior written consent to an alternative arrangement.

2.11. The Supplier shall ensure that any device which is used to process Buyer's Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security> and <https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles>.

2.12. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer's Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation. The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

2.13. When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer's Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of company premises. The term 'under cover' means "that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings".

2.14. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier's assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier's organisation in line with paragraph 2.15.

2.15. In the event of termination, equipment failure or obsolescence, all Buyer's Data and Buyer's Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC-approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-contractor protects) the Buyer's Information and Buyer's Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

2.16. Access by Supplier Staff to Buyer's Data, including user credentials, shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Buyer. All Supplier Staff must complete this process before access to Buyer's Data is permitted.

2.17. All Supplier Staff who handle Buyer's Data shall have annual awareness training in protecting information.

2.18. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the Services delivered. If an ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant business continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

2.19. Any suspected or actual breach of the confidentiality, integrity or availability of Buyer's Data, including user credentials, used or handled in the course of providing the Services shall be recorded as an incident. This includes any non-compliance with the Departmental Security Standards and these provisions, or other security standards pertaining to the solution.

Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the Supplier should provide an explanation about the delay.

Incidents shall be reported through the Buyer's nominated system or service owner.
Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

2.20. The Supplier shall ensure that any IT systems and hosting environments that are used to handle, store or process Buyer's Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work is to be carried out. In the event of significant security issues being identified, a follow up remediation test may be required, as determined by the Buyer upon review of the ITHC findings.

2.21. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process, or store Buyer's Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.

2.22. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the Services being supplied and the Supplier's, and any sub-contractors', compliance with the paragraphs contained in this Appendix.

2.23. The Supplier and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the Buyer. This will include obtaining any necessary professional security resources required to support the Supplier's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

2.24. Where the Supplier is delivering an ICT solution to the Buyer they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Buyer's Policy. The Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer's expectation is that the Supplier shall provide written evidence of:

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.

- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Supplier shall provide details of who the awarding body or organisation will be and date expected.

Additional information and evidence to that listed above may be required to ensure compliance with DfE security requirements as part of the DfE security assurance process. Where a request for evidence or information is made by the Buyer, the Supplier will acknowledge the request within 5 working days and either provide the information within that timeframe, or, if that is not possible, provide a date when the information will be provided to the Buyer. In any case, the Supplier must respond to information requests from the Buyer needed to support the security assurance process promptly and without undue delay.

2.25. The Supplier shall contractually enforce all the Departmental Security Standards and these provisions onto any third-party suppliers, sub-contractors or partners who could potentially access Buyer's Data in the course of providing the Services.

2.26. The Supplier shall comply with [the NCSC's social media guidance: how to use social media safely](#) for any web and social media-based communications. In addition, any Communications Plan deliverable must include a risk assessment relating to the use of web and social media channels for the programme, including controls and mitigations to be applied and how the NCSC social media guidance will be complied with. The Supplier shall implement the necessary controls and mitigations within the plan and regularly review and update the risk assessment throughout the contract period. The Buyer shall have the right to review the risks within the plan and approve the controls and mitigations to be implemented, including requiring the Supplier to implement any additional reasonable controls to ensure risks are managed within the Buyer's risk appetite.

2.27. Any Supplier ICT system used to handle, store or process the Buyer's Data, including any Supplier ICT systems connected to systems that handle, store or process the Buyer's Data, must have in place protective monitoring at a level that is commensurate with the security risks posed to those systems and the data held. The Supplier shall provide evidence to the Buyer upon request of the protective monitoring arrangements in place needed to assess compliance with this requirement.

Appendix 1 G-Cloud 14 Service Definition

T R I B A L



Course Directory Service - Service Definition

G-Cloud 14



Appendix 2 G-Cloud 14 Service Pricing



NCS Course Directory Service Delivery

Proposal 11

February 2025

