Crown Commercial Service

G-Cloud 10 Call-Off Contract

This Call-Off Contract for the G-Cloud 10 Framework Agreement (RM1557.10) includes: Part A - Order Form ..... **Error! Bookmark not defined.**

Part A - Order Form

Digital Marketplace service ID number:	748988642215825
Call-Off Contract reference:	CCSO19A28
Call-Off Contract title:	Assessment Capability Tool for the CMTA Programme

Call-Off Contract description:	Provision of licences, hosting and platform support for the application of Assessment Management Platform (CMAP). The Supplier will provide an ongoing assessment capability tool for the Contract Management Training and Accreditation (CMTA) programme for a twelve (12) month term whilst a new Government Commercial Function digital platform is procured.
Start date:	08th July 2019
Expiry date:	07th July 2020
Call-Off Contract value:	£50,870.00 (Excluding VAT)
Charging method:	REDACTED TEXT
Purchase order number:	REDACTED TEXT

This Order Form is issued under the G-Cloud 10 Framework Agreement (RM1557.10).

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 Deliverables 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	Cabinet Office REDACTED TEXT

To: the Supplier	MatsSoft Limited, REDACTED TEXT
Together: the 'Parties'	

Principle contact details

For the Buyer:	REDACTED TEXT
For the Supplier:	REDACTED TEXT

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 08th July 2019 and is valid for twelve (12) months, expiring 07th July 2020.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least ninety (90) Working Days from the date of written notice for disputed sums or at least thirty (30) days from the date of written notice for Ending without cause.
Extension period:	There are no extension options.

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:	This Call-Off Contract is for the provision of Services under:

	Lot 2 – Cloud Software
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: Provision of licences, hosting and platform support for the application of Assessment Management Platform (CMAP) previously supplied by Supplier via Mott MacDonald. The following will be included in this Contract: MATS Low-Code Platform – Professional edition • Twenty (20) x Full User Licences • Four Hundred and Fifty (450) x Application Subscriber Licences Hosting for one (1) x Applications, environment limited to: 2 vCPU, 4GB RAM, 256GB storage, 512GB EBS Snapshot, 230GB/month data transfer; Accreditation Management Platform (CMAP) In addition, the customer requires: REDACTED TEXT
Additional services:	Not Applicable
Location:	REDACTED TEXT
Quality standards:	The Quality standards required for this Call-Off Contract are as per the Supplier's Digital Marketplace listing: https://www.digitalmarketplace.service.gov.uk/gcloud/services/748988642215825 Including, but not limited to: Cyber Essentials - Please see also Annex A - Security Management of this Contract Order Form [TBD]
Technical standards:	The technical standards required for this Call-Off Contract are as per the Digital Marketplace listing: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/748988642215825
Security standards:	As part of the Security standards required for this Call-Off Contract please refer to Annex A - Security Management, of this Contract Order Form.

Service level agreement:	REDACTED TEXT
Onboarding:	The onboarding plan for this Call-Off Contract is set out in the applicable Supplier's service definition.
Offboarding:	At the end of the contract, the Supplier will provide appropriate technical resources and support the export of the content from CMAP Platform. The Supplier will provide an Exit plan as per Clause 21.1 to 21.8. The off boarding plan for this Call-Off Contract is set out in the Supplier's Services definition.
Collaboration agreement:	Not Applicable.
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other defaults will not exceed the greater 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance:	The insurance(s) required will be: ● A minimum insurance period of six (6) years following the expiration or Ending of this Call-Off Contract; ● Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law); ● Employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than ten (10) consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: All Framework audit provisions Clauses 7.3 to 7.12.
Buyer's responsibilities:	The Buyer is responsible for ensuring payment of all invoices in full as per the Call-Off charges and Payments section of this Call-Off Contract. Full User and/or Application Subscriber user accounts may not be operated by any form of computerised or robotic means. A user subscription to the CMAP may not be used by more than one individual unless it has been transferred in its entirety to another individual, in which case the prior user shall no longer have any right to access or use the CMAP. The number of users that may use the CMAP is limited to the number as specified in this

	agreement. Each user shall keep a secure password for their use of the CMAP and that each user shall keep their password confidential. Use of the CMAP is solely for purposes connected with Customer's own business which for clarity shall not permit Customer to use the CMAP to process data for third parties on a commercial basis nor shall permit Customer to provide a bureau service (i.e. a business service) to a third party. Customer will implement security policies in line with good industry practice. Customer controls what data is provided to the CMAP for the purposes of the provision of the CMAP and how such data is transferred to and from the CMAP. Customer shall not willingly or recklessly circumvent or disable any security features or functionality associated with the CMAP. Customer shall not use the CMAP in any manner prohibited by law. Customer is responsible for provisioning, configuring and maintaining any infrastructure, systems and/or software required to access and/or interact with the CMAP. In particular: o Customer is responsible for providing and maintaining all direct or indirect connectivity with the appropriate bandwidth to the Supplier data centres from which the CMAP is provided. o Appropriate bandwidth is required to support access to the CMAP by Customer staff, and as such, connectivity to the Customer LAN will also need to be enabled by Customer. Customer hereby acknowledges that prior to it implementing any new release of the CMAP it is responsible for testing that any applications that operate in relation to the CMAP will not be affected by implementing such release.
Buyer's equipment:	Not Applicable – this is cloud-based service provision.

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 through BACS.
Payment profile:	The payment profile for this Call-Off Contract is Annual Payments payable in advance.
Invoice details:	The Supplier will issue electronic invoices annually. The Buyer will pay the Supplier within (30) days of receipt of a valid invoice.

Who and where to send invoices to:	Invoices will be submitted to: REDACTED TEXT Electronic invoices will be submitted to: REDACTED TEXT
Invoice information required	All invoices must include: - A valid Purchase Order (PO) number; - Contract Reference; - A Transparent Breakdown of Costs.
Invoice frequency:	Invoice will be sent to the Buyer on an annual basis to: REDACTED TEXT
Call-Off Contract value:	The total value of this Call-Off Contract is £50,870.00 (Excluding VAT)
Call-Off Contract charges:	The breakdown of the Charges is: <u>Solution - £48,630.00 per annum (excluding VAT)</u> MATS Low-Code Platform – Professional edition ● Twenty (20) x Full User Licences ● Four Hundred and Fifty (450) x Application Subscriber Licences Hosting for one (1) x Applications; • Accreditation Management Platform (CMAP) • Environment limited to: 2 vCPU, 4GB RAM, 256GB storage, 512GB EBS Snapshot, 230GB/month data transfer <u>Professional Services - £2240.00 (excluding VAT) one off cost</u> REDACTED TEXT

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones: • All details of the Onboarding and Offboarding requirements as above in the Onboarding and Offboarding section. • Any support issues to be resolved as per the Supplier's Service Level Agreement. Implementation and Setup completed with one (1) week of Contract Award.
Guarantee:	Not Applicable

Warranties, representations:	Not Applicable
Supplemental requirements in addition to the Call-Off terms:	Not Applicable
Alternative clauses:	Not Applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms:	• Please see Annex A – Schedule B Security Management • The parties agree that there are no Project Specific IPRs in the Services. • In the event that any software is created for Customer under this Call-Off Contract it is agreed that it will not be suitable for publication as open source.
Public Services Network (PSN):	Not Applicable
Personal Data and Data Subjects:	Will Schedule 7 – Processing, Personal Data and Data Subjects be used: Yes

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 and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.10.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:		
Title:		

Signature:		
Date:		

Schedule 1 – Services

Provision of licences, hosting and platform support for the application of Assessment Management Platform (CMAP).

MATS Low-Code Platform – Professional edition

- Twenty (20)) x Full User Licences
- Four Hundred and Fifty (450) x Application Subscriber Licences

Hosting for one (1) x Applications;

- Accreditation Management Platform (CMAP)
- Environment limited to: 2 vCPU, 4GB RAM, 256GB storage, 512GB EBS Snapshot, 230GB/month data transfer

In addition, the customer requires:

REDACTED TEXT

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) cannot be amended during the term of the CallOff Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Solution - £48,630.00 per annum (excluding VAT)

MATS Low-Code Platform – Professional edition

- Twenty (20) x Full User Licences
- Four Hundred and Fifty (450) x Application Subscriber Licences

Hosting for one (1) x Applications;

- Accreditation Management Platform (CMAP)

REDACTED INFORMATION					

Professional Services - £2240.00 (excluding VAT) one off cost

REDACTED TEXT

REDACTED INFORMATION				

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 24 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, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

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 extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses 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:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.2 to 5.3 (Force majeure)
- 5.6 (Continuing rights)
- 5.7 to 5.9 (Change of control)
- 5.10 (Fraud)
- 5.11 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)

- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- a reference to 'CCS' will be a reference to 'the Buyer'
- 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 Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.

2.4 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:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- 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 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 14digit 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:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Call-Off Contract terms
- have raised all due diligence questions before signing the Call-Off Contract
- have entered into the Call-Off Contract relying on its 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 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:

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

- a broker's verification of insurance
- receipts for the insurance premium
- 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:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 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 the Data Protection Legislation or under incorporated Framework Agreement clauses 8.83 to 8.91. 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 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royaltyfree licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown 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:

- rights granted to the Buyer under this Call-Off Contract
- Supplier's performance of the Services
- use by the Buyer of the Services

11.6 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:

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

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

11.7 Clause 11.5 will not apply if the IPR Claim is from:

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, 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:

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

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- 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

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

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

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

13.3 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 policy and all Buyer requirements in the Order Form.

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

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

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protectionsensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
- 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, available at https://www.gov.uk/government/publications/technology-code-of-practice/technologycode-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

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

13.7 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.

13.8 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.

13.9 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 available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-codeof-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 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:

- 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
- 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 CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer 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, available at https://www.ncsc.gov.uk/guidance/10-stepscyber-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:

- an executed Guarantee in the form at Schedule 5
- 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:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers 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:

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- any fraud

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

- an Insolvency Event of the other Party happens
- 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:

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- 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); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and
  8.92 to 8.93 (Waiver and cumulative remedies)
- 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:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- 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
- 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
- work with the Buyer on any ongoing work
- 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	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by PDF to the correct email address without getting an 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 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 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 extend the Term beyond 24 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 GDS 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:

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- 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:

- 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
- 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
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- 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:

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- 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 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form

- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

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:

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

- comply with Buyer requirements for the conduct of personnel

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

- 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 isn't 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:

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- 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 co-operate 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:

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

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

29.8 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:

- work proactively and in good faith with each of the Buyer's contractors
- 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 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. 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 CallOff Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only Processing the Supplier is authorised to do is

listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional Processing if permitted by Law).

33.2 The Supplier will assist the Buyer with the preparation of any Data Protection Impact Assessment required by the Data Protection Legislation before commencing any Processing (including provision of detailed information and assessments in relation to Processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.

33.3 The Supplier must have in place Protective Measures, details of which shall be provided to the Buyer on request, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier staff with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier's obligations under this Clause;

ii) are subject to appropriate confidentiality undertakings with the Supplier

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

33.5 The Supplier will not transfer Personal Data outside of the European Union unless the prior written consent of the Buyer has been obtained, which shall be dependent on such a transfer satisfying relevant Data Protection Legislation requirements.

33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

33.7 The Supplier will notify the Buyer without undue delay if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation, and insofar as this is possible, in accordance with any timescales reasonably required by the Buyer

33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

i) the Buyer determines that the Processing is not occasional;

ii) the Buyer determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) 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 Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● 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 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.
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 endto-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	Data, personal data and any information, which may include (but isn't limited to) any: ● 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 Data Protection Legislation.
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	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing by the Processor under this Call-Off Contract on the protection of Personal Data.
Data Protection Legislation	Data Protection Legislation means: i) the GDPR, the LED and any applicable national implementing Laws 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, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Takes the meaning given in the Data Protection Legislation.

Default	Default is any: ● 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 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.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
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 outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most upto-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● 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 The following do not constitute a Force Majeure event: ● 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 ● 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 RM1557.10 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 CallOff 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 Section 2 (Services Offered) 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.
GDPR	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.

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.
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	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.

Intellectual Property Rights or IPR	Intellectual Property Rights are: ● 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 ● 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 ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	A 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 knowhow already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.

Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '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 section 6 (What you report to CCS).
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.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	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: ● 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: ○ 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: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's highperformance 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).
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 GCloud Services, including backup 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 Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
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/spendcontrols-check-if-you-need-approval-to-spend-money-on-aservice
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 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.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

iii) the Buyer determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

33.9 Before allowing any Sub-processor to Process any Personal Data related to this Call-Off Contract, the Supplier must:

i. notify the Buyer in writing of the proposed Sub-processor(s) and obtain its written consent;

ii. ensure that it has entered into a written agreement with the Subprocessor(s) which gives effect to obligations set out in this Clause 33 such that they apply to the Sub-processor(s); and

iii. inform the Buyer of any additions to, or replacements of the notified Sub-processors and the Buyer shall either i) provide its written consent or ii) object.

33.10 The Buyer may at any time put forward a Variation request to amend this Call-Off Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-andlegal-documents

Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-and-legaldocuments

Schedule 5 - Guarantee

The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legaldocuments

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Schedule 7 - Processing, Personal Data and Data Subjects

Subject matter of the processing:
Personal data of participants who are assessed using the CMAP Application will be processed.

Duration of the processing:
The Contract Management Capability Programme (CMCP) will keep user personal data for their length of employment in a government department and up to 7 years after leaving the Civil Service.

Nature and purposes of the Processing:
CMAP user personal data will be collected and kept in order for the Contract Management Capability Programme (CMCP) to engage, develop and accredit individuals involved in contract and supplier management activities. User data will also be used to develop an appropriate training and accreditation offer for contract managers.

The CMCP will use data to contact users about relevant training and accreditation and networking events. CMCP will keep records of user personal development and talent conversations to further provide assistance regarding talent and career planning.

Type of Personal Data:
The CMCP will process the following personal data:

- name
- email address
- job title
- department
- business unit/directorate
- primary career anchor
- contracts connected with and activities around contract and supplier management

Categories of Data Subject:
The categories of users related to the CMAP application include Assessors, Participants and Moderators.

Plan for return or destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data:
All user data that is stored and processed by CMAP and stored by the supplier and their agents will be digitally delivered to the CMCP team on request or at the cessation of this contract. At the cessation of the contract, and subsequent to providing the user data in a digital format to the CMCP Team, all user data retained by the supplier will be totally and irrevocably erased.

Annex A

Schedule B
Security Management

Definitions In this Schedule:

Authority	is The Cabinet Office – the "Buyer" as defined in the Call-Off Contract
Authority Data	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: a. supplied to the Supplier by or on behalf of the Authority; and/or b. which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Data Controller;
Breach of Security	an event that results, or could result, in:

(c) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or

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

Certification Requirements	means the information security requirements set out in Paragraph 5 of Schedule B (Security Management);
CHECK Service Provider	means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC services required by the Para graph 6.2 of Schedule B (Security Management);
Core Information Management System	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources, which the Authority has determined in accordance with Paragraph Error! Reference source not found.;
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with Paragraph 3 of Schedule (Security Management) using the template set out in Annex 2 to Schedule B (Security Management);
Information Management System	comprises: (i) the Supplier Equipment; (ii) the Supplier System; and (ii) the Sites at which Authority Data;

Information Security Approval Statement	a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Authority: (i) is satisfied that the identified risks have been adequately and appropriately addressed; and (ii) the Supplier may use the Information Management System to Process Authority Data;
Information Assurance Assessment	is the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 3 of Schedule B (Security Management) in order to manage, mitigate and, where possible, avoid information security risks including cyber attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Annex 2 to Schedule B (Security Management);
Information Security Management Document Set	comprises: (i) the Information Assurance Assessment; (ii) the Personal Data Processing Statement; (iii) the Required Changes Register; and, (iv) the Incident Management Process, which shall be prepared by the Supplier using the templates set out in Annex 2 to Schedule B (Security Management);
ITHC	has the meaning given in Paragraph 6.1 of Schedule B (Security Management);
Personal Data	has the meaning given in the Data Protection Legislation;
Personal Data Breach	has the meaning given in the Data Protection Legislation;
Personal Data Processing Statement	sets out: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 3 of Schedule

	B (Security Management) and included in the Information Security Management Document Set ;
Process Authority Data	any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Authority Data;
Protective Measures	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it
Required Changes Register	is the register within the Information Security Management Document Set which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Information Security Management Document Set as a consequence of the occurrence of any of the events set out in Paragraph 4.2 of (Security Management) together with the date by which such change shall be implemented and the date on which such change was implemented;
Risk Register	is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Authority for approval in accordance with Paragraph 3 of Schedule B (Security Management);
Sites	comprise: (i) those premises from which the Services are to be provided; (ii) those premises from which Supplier manages, organises or otherwise administers the provision of the Services; and, (iii) those premises at which any Supplier Equipment or any party of the Supplier System is located.

Supplier Equipment	the hardware, computer and telecoms devices and equipment used by the Supplier or its Subcontractors (but not hired, leased or loaned from the Authority) for the provision of the Services;
Supplier System	the information and communications technology system used by the Supplier in implementing and performing the Services, including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);

1. Introduction

1.1 This Schedule addresses:

1.1.1 the arrangements which the Supplier shall implement and comply with when performing its obligations under this Agreement and/or providing the Services in order to ensure the security of the Authority Data and the Information Management System;

1.1.2 the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;

1.1.3 The security requirements in Annex 1 to this Schedule which the Supplier must comply with;

1.1.4 the tests which the Supplier shall conduct on the Information Management System during the Term in Paragraph 6;

1.1.5 the Supplier's obligations to:

(a) return or destroy Authority Data on the expiry or earlier termination of this Agreement; and

(b) prevent the introduction of Malicious Software into the Service and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Services in Paragraph 8; and

(c) report Breaches of Security to the Authority.

2. Principles of Security

2.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

2.1.1 the Supplier System; 2.1.2 the CMAP Application

2.1.3 the Service.

2.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Authority Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

2.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors;

2.2.2 the security of the Information Management System.

2.3 The Supplier shall provide the Authority with access to members of its information assurance personnel to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

3. Information Security Approval Statement

3.1 The Supplier may not use the Information Management System to Process Authority Data unless and until:

3.1.1 the Supplier has conducted a CHECK IT Health Check of the Supplier System in accordance with Paragraph 6.1; and

3.1.2 the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 3.

3.2 The Supplier shall document in the Information Security Management Document Set how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule B and the Agreement in order to ensure the security of the Authority Data and the Information Management System.

3.3 The Supplier shall prepare and submit to the Authority within 20 Working Days of the date of this Agreement, the Annex B Information Security Management Document Set, which comprises:

3.3.1 an Information Assurance Assessment;

3.3.2 the Required Changes Register;

3.3.3 the Personal Data Processing Statement; and

3.3.4 the Incident Management Process.

3.4 The Authority shall review the Supplier's proposed Information Security Management Document Set as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

3.5 a Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or

3.6 a rejection notice which shall set out the Authority's reasons for rejecting the Information Security Management Document Set.

3.7 If the Authority rejects the Supplier's proposed Information Security Management Document Set, the Supplier shall take the Authority's reasons into account in the preparation of a revised Information Security Management Document Set, which the Supplier shall submit to the Authority for review within 10 Working Days or such other timescale as agreed with the Authority.

3.8 The Authority may require and the Supplier shall provide the Authority and its authorised representatives with: 3.8.1 access

to the Supplier Personnel;

3.8.2 access to the Information Management System to audit the Supplier and its Sub-contractors compliance with this Agreement; and

3.8.3 such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

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

4. Compliance Reviews

4.1 The Supplier shall regularly review and update the Information Security Management Document Set, and provide such to the Authority, at least once each year and as required by this Paragraph.

4.2 The Supplier shall notify the Authority within 2 Working Days after becoming aware of:

4.2.1 a significant change to the components or architecture of the Service;

4.2.2 a new risk to the components or architecture of the Service;

4.2.3 a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph 9.2 of Annex 1 to this Schedule;

4.2.4 a change in the threat profile;

4.2.5 a significant change to any risk component;

4.2.6 a significant change in the quantity of Personal Data held within the Service;

4.2.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

4.2.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

Within 10 Working Days of such notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Authority for review and approval.

4.3 Where the Supplier is required to implement a change, including any change to the Information Management System, in order to remedy any non-compliance with this Agreement, the Supplier shall effect such change at its own cost and expense.

5. Certification Requirements

5.1 The Supplier shall be, and shall ensure that each Sub-contractor which Processes Authority Data is, certified as compliant with:

The Supplier's solution shall be Cyber Essential Plus or be willing to obtain this certification within an agreed timescale as agreed with the Authority.

5.2 The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

5.2.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

5.2.2 are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

5.3 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.

5.4 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

5.4.1 immediately ceases using the Authority Data; and

5.4.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph.

6. Security Testing

6.1 The Supplier shall, at a reasonable charge to the Authority procure and conduct:

6.1.1 an IT Health CHECK ("ITHC") of the Supplier System by a CHECK Service Provider; and

6.1.2 such other security tests as may be required by the Authority and which are set out in this Agreement,

The Supplier shall complete all of the above security tests before the Supplier submits the Information Security Management Document Set to the Authority for review in accordance with Paragraph 3; and it shall repeat the ITHC not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with this Paragraph.

6.2 In relation to each ITHC, the Supplier shall:

6.2.1 agree with the Authority the aim and scope of the ITHC;

6.2.2 promptly, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

6.2.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for approval by the Authority (each a "Vulnerability Correction Plan") which sets out in respect of each vulnerability identified in the IT Health Check report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied;

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

6.3 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

6.4 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within 2 days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Authority with a copy of the test report and:

6.4.1 propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and

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

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

6.6 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Annex 1 to this Schedule. 7. Security Monitoring and Reporting

7.1 The Supplier shall:

7.1.1 monitor the delivery of assurance activities;

7.1.2 maintain and update the Information Security Management Document Set in accordance with Paragraph 4;

7.1.3 agree a document which presents the residual security risks to inform the Authority's decision to give approval to the Supplier to process, store and transit the Authority's data;

7.1.4 monitor security risk impacting upon the operation of the Service;

7.1.5 report Breaches of Security in accordance with the approved Incident Management Process;

7.1.6 agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 30 days of the date of this Agreement.

8. Malicious Software

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

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

8.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 8.2 shall be borne by the parties as follows:

8.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

8.3.2 by the Authority, in any other circumstance.

9. Breach of Security

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

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

9.2.1 Immediately take all reasonable steps necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure;

9.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

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

Annex 1: Security Requirements

REDACTED TEXT

Annex B: Information Security Management Document Set Template

REDACTED TEXT Executive Summary

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any residual risks that need acceptance by the Authority. This should be completed at the end of the assurance process.>

List of Contents

Change History

Version Number	Date of Change	Change made by	Nature and reason for change

References, Links and Dependencies

This document is dependent on the supporting information and assurance provided by the following documents.

ID	Document Title	Reference	Date

Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

Contractual Arrangements

< Please provide detail of how the system/product/service has been procured including what contracts (service model, call-off, framework, security schedules) are in place.>

Governance, reporting and accountability

<Include a list of the lead security roles for the project and the reporting structures/decision making process for the security work.>

Customers

< Include list of participating departments/organisations if appropriate and known.>

Information Assurance Assessment

Data/Information

<Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

Overview of technical architecture

< In this section, please provide an architectural diagram of the system. A brief explanation of the relevant components should be included.>

Logical Data Flow Diagram

< Include a diagram of the logical data flows. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service.>

Third Party Suppliers

< Include a list/table of the Suppliers, what function they perform, what data they store/process and what assurance activities/due diligence activities have been taken place. Also, include evidence of compliance with ISO 27001:2013 or Cyber Essential/Cyber Essential Plus. Please ensure that the service/system or product that you are procuring is included in the scope of certification>

Location of data processing, storage, transfer, back-up tapes

< This section to include third party suppliers>

Off Shoring

< Please provide detail of any off-shoring arrangements/location, including third party suppliers. Please specify what products, systems, data will be off-shored and where. Also include any detail of what assurance and due diligence has taken place.>

Risk Management

< Include a short explanation for what methodology will be used to assess risks to this system/service/product. Have you used a formal methodology or an informal? Please note that advice on risk management can be found via this link: https://www.ncsc.gov.uk/guidance/risk-management-collection.>

Risk Register

<This section to include a table containing a prioritised risk list which contains the output from the risk assessment and lists technical, personnel, physical and procedural controls that are being implemented to mitigate those risks. An example table is shown below. Any significant residual risks should be agreed with the Authority/Customer and included in the Executive Summary of this document.>

Risk ID	Risk Description	Vulnerability	Untreated Risk Level	Security Controls	Residual Risk Level
R1	Internet attackers could hack the system.	The service systems are exposed to the internet via the web portal.	High	Internet-facing firewalls Internet-facing IP whitelist Protective monitoring Application access control Anti-virus for incoming files Patching	Low

Security controls

< Provide a short explanation of the security controls relied upon to treat the risks in the Risk Register.>

Table of Hardware and Software relevant to the service

<This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

Incident Management Process

<The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

Required Changes Register

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

Personal Data Processing Statement

<This should include: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach.>

Annex A. ISO 27001:2013 and Cyber Essential Plus certificates

Annex B. Cloud Security Principles assessment (a spreadsheet may be attached).

Annex C. Protecting Bulk Data assessment if required by the Authority/Customer (a spreadsheet may be attached).

Annex E. Latest ITHC report and Vulnerability Correction Plan