Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form

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

Platform service ID number	328173153148861
Call-Off Contract reference	CCSO22A25
Call-Off Contract title	The Provision of GDS assessments for CAS
Call-Off Contract description	Contract Award Service (CAS) is currently in its GDS private beta phase, in usage by a group of beta users. Cognizant will identify activities necessary to bring the service to a standard where it can pass the GDS private beta assessment and provide a delivery plan for these activities. Cognizant will then execute user-centred design activities within the plan and manage the overall delivery of the plan.
Start date	9th December 2022
Expiry date	31st March 2023
Call-Off Contract value	£475,000.00

Charging method	BACS
Purchase order number	TBC

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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

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

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

From the Buyer	Crown Commercial Service **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**.

To the Supplier	Cognizant Worldwide **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**. **REDACTED TEXT under FOIA Section 40, Personal Information**.
Together the 'Parties'	

Principal contact details

For the Buyer:

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

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

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

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

For the

Supplier:

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

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

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

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

Call-Off Contract term

Start date	This Call-Off Contract Starts on **9th December 2022** and is valid for **4 months**.
Ending (termination)	The notice period for the Supplier needed for Ending the CallOff Contract is at least **[90]** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **[30]** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	N/A

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 3: Cloud support

G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: • Business and technology analysis and alignment • Flexible delivery approach including lean agile, scrum and GDS model • Digital and transformation road-mapping • Digital and transformation road-mapping planning, development, design and automation services
Additional Services	**N/A**
Location	The Services will be delivered to **remote delivery**
Quality Standards	The quality standards required for this Call-Off Contract are **Staff security clearance - Conforms to BS7858:2019** **Government security clearance - Up to Security Check (SC). Standard clearance is BPSS.**
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are: ISO/IEC 27001 certification ISO 22301- Business Continuity Management System

<table>
<tr>
<td>Service level agreement:</td>
<td>The service level and availability criteria required for this Call-Off Contract are:
<table>
<tr><th>Service Area</th><th>SLA description</th><th>Target</th></tr>
<tr><td>Supplier performance</td><td>Adherence to key milestones set out in Section 7 and the Statement of Work (SOW).</td><td>100% delivery before or on delivery milestone date.</td></tr>
<tr><td>Contract Management</td><td>Attendance at the monthly Contract Review meeting as described in section 17.</td><td>Monthly

100%</td></tr>
<tr><td>Contract Management</td><td>onthly Update Note sent to the Contract Manager within 4 working days of a Monthly Contract Review Meeting</td><td>Monthly

100%</td></tr>
<tr><td>Invoicing/Billing</td><td>Compliant and fully transparent breakdown in costs and shall accurately reflect the services provided.

Frequency: monthly in arrears</td><td>100%</td></tr>
<tr><td>Reporting</td><td>Management reporting to 100% accuracy submitted on time as detailed in section 8.

Frequency: monthly</td><td>100%</td></tr>
<tr><td>Replacement of key personnel</td><td>Notification at the contract management review meeting with the contract manager.</td><td>TBA through contracting discussions.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Onboarding</td>
<td>N/A</td>
</tr>
</table>

Offboarding	N/A
Collaboration agreement	N/A
Limit on Parties' liability	The parties agree that the below limits of liability will apply in regards to the delivery of these services: The annual total liability of either Party for all Property Defaults will not exceed 125%. 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 of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance	The Supplier insurance(s) required will be: ● a minimum insurance period of 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

Buyer's responsibilities	N/A
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	N/A

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 **BACS**
Payment profile	The payment profile for this Call-Off Contract is **monthly** in arrears.

Invoice details	The Supplier will issue electronic invoices **monthly** in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Invoices will be sent to **REDACTED TEXT under FOIA Section 40, Personal Information**.
Invoice information required	All invoices must include the following: Purchase Order number, detailed and transparent breakdown of charges, contract reference number, key company details, dates, project reference.
Invoice frequency	Invoices will be submitted monthly in arrears.
Call-Off Contract value	The total value of this Call-Off Contract is £475,000.00
Call-Off Contract charges	**REDACTED TEXT under FOIA Section 43 Commercial Interests.** **REDACTED TEXT under FOIA Section 43 Commercial Interests.** Total £475,000

Additional Buyer terms

Performance of the Service	Phase 1 – Set up for success – 4.5 weeks 21/11/2022 – 21/12/2022 Phase 2a – GDS Assessment preparation part 1 – 13 weeks – 03/01/2023-31/03/2023

Warranties, representations	Any IPR created by this engagement will solely rest with CCS.
Supplemental requirements in addition to the Call-Off terms	Within the scope of the Call-Off Contract, the Supplier will ensure all relevant documentation is provided to CCS , together with the associated knowledge transfer activities as directed by CCS to the delivery partner for each work package
Personal Data and Data Subjects	Annex 1

1. Formation of contract

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

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

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

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

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13

.

Signed	Supplier	Buyer

Name	**REDACTED TEXT under FOIA Section 40, Personal Information**.	**REDACTED TEXT under FOIA Section 40, Personal Information**.
Title	**REDACTED TEXT under FOIA Section 40, Personal Information**.	**REDACTED TEXT under FOIA Section 40, Personal Information**.
Signature	**REDACTED TEXT under FOIA Section 40, Personal Information**.	**REDACTED TEXT under FOIA Section 40, Personal Information**.
Date	Feb 13, 2023	Feb 21, 2023

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

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)

- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)

- 25 (Publicity and branding)

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

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

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

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

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

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

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

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

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

7.4 If specified in the Order Form, the Supplier will accept payment for G-

Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

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

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

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

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

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums

to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause

18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must

notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

9.2.2 the third-party public and products liability insurance contains an

'indemnity to principals' clause for the Buyer's benefit

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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:

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;

(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

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

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policyframework and the Government Security Classification policy: https:/www.gov.uk/government/publications/governmentsecurityclassifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-riskmanagementapproach and Protection of

Sensitive Information and Assets: https://www.cpni.gov.uk/protectionsensitive-information-and-assets

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

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technology-code-ofpractice/technology-code- of-practice

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the

Supplier, unless a shorter period is specified in the Order Form. The
Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)

- 24 (Liability); and incorporated Framework Agreement clauses:
  4.1 to 4.6, (Liability),

24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to

serve notice except if this CallOff Contract states otherwise.

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own

governance process. Where the Buyer is a central government department, this includes the need to obtain approval from 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:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses

4.1 to 4.6, the Supplier's liability:

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

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

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the

Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause

24.2 will not be taken into consideration.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the

Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to

End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period

29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29. 2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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.

29.3 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.

29.4 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.

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

29.5.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and GCloud 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 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

PURPOSE

CCS began the SCALE programme in Summer 2021, which incorporates the Contract Award Service (CAS). CAS aims to deliver a new platform to standardise and modernise the end-to-end procurement journey for buyers and suppliers across the 100+ commercial framework agreements that CCS operates. CAS has now launched in Beta form to real users for 3 of the key framework agreements (DSP, GCloud, and DOS) with one further agreement due to go live before end of year (MCF). CCS now need to take CAS through a GDS Private Beta phase, to validate that activity to date has been conducted in a way that meets GDS standards. The scope of this engagement is for Cognizant to provide UCD support to help CCS pass the GDS Private Beta Assessment.

1.1 The requirements are being sourced from the GCLOUD13 commercial agreement using the Contract Award Digital service based on the outcomes required to fulfil this ask.

The supplier shall be accountable for the full outcomes set within this contract CCS will provide the internal assurance management roles of Head of Portfolio delivery Claire.pagett, Project Management,james.grigg akos.Nwachukwu Product Management Jack Foulkes, and Architecture Nick Openshaw. However these roles will not be responsible for any outcomes detailed within this document and be supporting roles only.

All additional roles to fulfil the outcome MUST come from the delivery partner to ensure that the outcomes set within this contract are delivered on time. Failure to deliver the outcomes will be subject to CCS penalties which will be detailed further in this document.

Data Digital Services is directly accountable for the delivery of the outcomes set out in this document into the CCS Business. .

CCS shall hereafter be referred to as the Contracting Authority.

BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

The outcome based deliveries within this document have been broken down into Work Packages Phases for delivery these are as follows:

Work Package	Title	Description

Phase 1	Onboarding & Planning	• Onboard our new team, familiarise with work-to-date • Set-up ways of working • Assess scope of work required to get to beta assessment readiness
		• Align with GDS • Create a detailed plan outlining activities needed to successfully pass an assessment and timeline and resources required for delivering them
Phase 2a	GDS Assessment Preparation part 1 – Jan to March	• Advise on creation of KPI dashboard for CAS live usage data • Detailed UX review of as-built service, identifying possible usability issues and forming into a prioritised Backlog • Create Service Blueprint of the as-built service • Update CAS Figma documen- tation to include all page views, high level page flows and updated components • Plan and execute user re-search with a target of 72 user participants across 4 frameworks • User survey created, circulated and results analysed • Findings report from user testing • Set up multi-disciplinary sprint team combining Cognizant team with engineering and QA Testing resources • Set up appropriate ways of working for Sprint team • Create prioritised JIRA ticket backlog

		• Deliver 2x two week sprints of product iteration based on Backlog tickets
	GDS Assessment Preparation part 2 – April to May **(NOTE THIS IS NOT IN SCOPE OF THIS CON-TRACT)**	• Manage and provide UCD resources to Sprint team for delivery of two further sprints of 2 • weeks of product iteration Preparation for GDS assessment – collecting all service documentation into presentable and shareable form and preparing assessment materials (excluding technical documentation and materials which will be provided by CCS) • Conduct handover to CCS design team to allow them to take
		over on continuous design improvement of CAS platform GDS Assessment is scheduled to take place on week commencing **22nd May 2023)** and subject to a six week lead time for booking - this must be agreed and in place by **10th April 2023**

DELIVERY,GOVERNANCE, SUPPORT

The Supplier will be accountable for the team formation and required digital expertise (including tools) to deliver the outcomes set in this document.

The Supplier shall work with:

The Head of Portfolio (**REDACTED TEXT under FOIA Section 40, Personal Information)** to enable reporting to the CCS CEO and Executive Board members The Data and Digital services CDIO, Deputy Director of Programme Portfolio & Improvement (**REDACTED TEXT under FOIA Section 40, Personal Information)** and Commercial Director (**REDACTED TEXT under FOIA Section 40, Personal Information**.)

The CCS Project Manager Manager (**REDACTED TEXT under FOIA Section 40, Personal Information**.) (**REDACTED TEXT under FOIA Section 40,**

Personal Information.) and the CCS in-house functions as detailed in this document, as part of the existing delivery methodology

Work closely with CCS business via the Project and Product Managers (**REDACTED TEXT under FOIA Section 40, Personal Information**.) to deliver the changes, aligning to CCS technical architecture standards and governance.

1.1.1 **Governance**

1.1.1.1 Regular meetings with a Governance Board to ensure progress is managed as expected.
1.1.1.2 Gateway Meetings will form part of improved governance processes. At each Gateway Meeting there will be a presentation of the latest plan, a summary of progress against the plan and an updated view on CCS's required input and project dependencies.
1.1.1.3 An open forum to discuss any changes required to improve delivery efficiency and confidence, these may include, CCS resource impacts and progress, team shape and any required changes, impact to the beta assessment date
1.1.1.4 Gateway Meetings will take place at the end of Phase 1, and then at 4 week intervals thereafter

1.1.2 **Project Support**

The Supplier shall on-board timely, capable resources to meet the delivery outcomes.

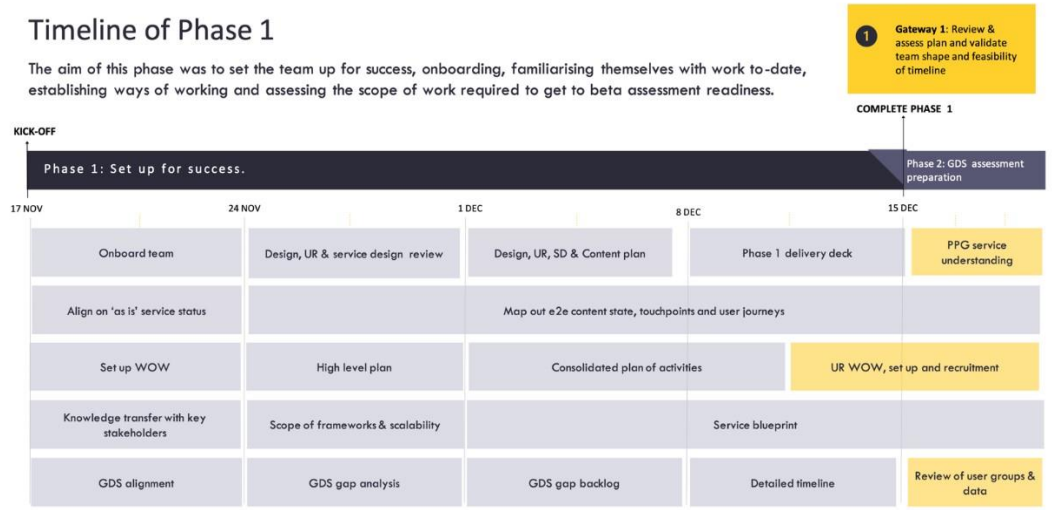
The Supplier shall ensure alignment to the GDS Service Standards applicable to GDS public beta assessment. How Beta Assessment Works provides full guidance on the approach and requirements ahead of the assessment

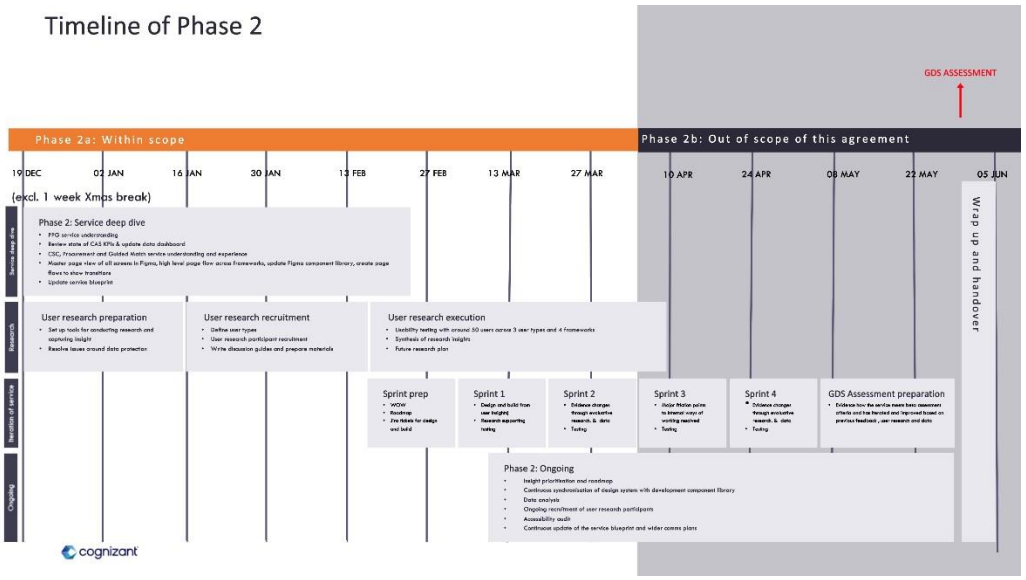
The Contracting Authority requires the immediate transfer and ownership of the intellectual property rights for any of the Supplier's work as part of this contract.

SCOPE, KEY MILESTONES, DELIVERABLES, TEAM STRUCTURE

Phase	Description	Duration	Start/End dates
1	Onboarding and planning	4.5 weeks	21/11/2022 - 21/12/2022

2	GDS Assessment preparation part 1	13weeks	03/01/2023 - 31/03/2023





Phase 2a Activity breakdown:

Detailed UX review of as-built service:

- Understand the wider service to demonstrate to assessment panel how the CAS works
- Update design system and design documentation to capture state of change since alpha and prepare for future iteration of design • Experience audit, data analysis and survey to understand existing use of CAS and inform areas to focus on during user sessions

User research:

- 72 proposition and usability testing sessions across the four frameworks to generate user insights and build roadmap of changes
- 18 users per framework at 6 users per user group
- Includes participants with accessibility needs - 1 hour 1:1 sessions

Sprint iterations:

- Starting once an initial roadmap based on user insights from the first framework has been created
- Two two-week sprints building evidence to show iteration of ways of working over time and iteration of the service based on user insights from ongoing data analysis and user testing
- Requires adjustment to existing ways of working as a multi- agency and multidisciplinary team to bring in additional disciplines
- Continue to communicate and work with wider service teams to improve CAS, maintaining a service blueprint for assessment panel and others
- Continue to update the CAS roadmap based on user insights to demonstrate plans for improvements

Team Shape: Phase 2

REDACTED TEXT under FOIA Section 40, Personal Information.

Dependencies

The following dependencies are prerequisites for Cognizant to deliver the specified outcomes and if they are not met the delivery of outcomes may be impacted

- There is a dependency on the CCS (and/or third party technical providers appointed by CCS) to ensure all technical requirements of the GDS standards can be met. Cognizant will assist this team to understand what is required and organise materials into presentable form, but is not responsible for creating content to meet technical aspects of standards
- Where our user research uncovers usability or technical issues with the asbuilt platforms it will be up to CCS and their third-party technical teams to deliver technical resolutions
- Where these issues are considered critical to passing beta assessment they must be released by CCS to Production code environments no later than 2 weeks before beta assessment date

- We will require CCS and third party technical teams engaged by CCS to provide access to instances and/or environments of CAS which we can use for user testing (we will need users to be able to complete user journeys within the service using test data and logins) access to these must be provided by latest two weeks before the scheduled start date of user research in our plan
- Access to category leads is significant part of research. They help identify user types, users of offline channels, and manage outgoing survey(s) to users. Cognizant will need two hours per week of time with category leads for the first two months of Phase 2
- Cognizant understand that CCS have implemented Google Analytics on Production environments and that user data is being collected – if this is not correct then we will not be able to provide usage data required to pass beta assessment
- Cognizant is relying on CCS to provide access to analytics and KPI dashboard in a timely manner
- We will require CCS content team to resolve content issues we discover during usability testing, resolution of content issues with CAS discovered during UX audit or user research is out of scope for the Cognizant content team
- CCS will perform a technical Accessibility Audit as this is one of the requirement for meeting the beta assessment standards. Findings will inform research sessions and complement the findings of accessibility sessions CCS will provide access to DPO in a timely manner to provide direction on DPIA requirements and any constraints around user research methods, tooling or GDPR restrictions
- Cognizant will require CCS assistance in recruiting users for user testing. CCS will be required to identify potential sources of users and send out recruitment invitations as drafted by Cognizant. Cognizant will make best endeavours to recruit sufficient user testing participants in order to meet beta assessment standards, however there is a dependency on CCS to either provide access to suitable users or enable us to provide cash incentives in order to recruit users via 3rd party recruiter

6.2 Individual Statement of Works will be agreed by CCS and the Delivery Partner to manage these elements.

MANAGEMENT INFORMATION/REPORTING

The Supplier shall provide the Contracting Authority with the following:

- Project plan
- Resource profiles;
- Progress and update reporting including forecasts/ actuals vs deliverables;
- Weekly progress reports including RAID
- Resolution reporting
- Adhoc reporting (as and when requested by the Contracting Authority)

CONTINUOUS IMPROVEMENT

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

The Supplier shall challenge and offer insights on greater efficiency to deliver Contract and Award Service components.

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

SUSTAINABILITY

Meetings will be held in the most effective format i.e. use of tech instead of face to face meetings where appropriate, provision of electronic report to prevent high paper usage.

The Supplier will be required to consider how Social Value has been considered in the development and implementation of the program as detailed in this specification.

The Supplier must consider their carbon footprint in allocating and deploying resources to undertake the requirement.

QUALITY

The Supplier shall ensure the capability of the team that delivers the services and adhere to the government profession standards:

Project Delivery capability framework

GDS Service Standards

How Beta Assessment Works Guidence

PRICE

Price shall be outcome based against contract deliverables, milestones and delivery of the agreed outcomes- Section 5.

Prices are to be submitted via Attachment 4 – Response Matrix excluding VAT and including all other expenses relating to Contract delivery.

1.2 The project plan and associated milestones will be used to assess supplier performance. Failure, by the supplier, to adhere to the agreed plan may impact the timing of milestone payments. Payments will only be approved upon full delivery and may be impacted in the event of delays.

1.3 The supplier is encouraged to maintain an open dialogue on project progress throughout the programme.

STAFF AND CUSTOMER SERVICE

The Supplier resources assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard. The Supplier shall provide the supporting evidence, if required, by the Contracting Authority.

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

The Supplier shall inform the Contracting Authority of All their key personnel names and contact details, including:

13.3.1. Account Manager

13.3.2 Delivery Lead

The Contracting Authority requires a minimum of 4 weeks' notice to any changes to the Delivery Partners' key personnel to be approved. The Supplier shall submit staff Biographies for approval by the Contracting Authority within the agreed timelines.

All Supplier staff are required to secure the minimum of Baseline Personnel Security Standard (BPSS) clearance to work on the Project and to access OFFICIAL Sensitive project information.

SERVICE LEVELS PERFORMANCE

The Authority will measure the quality of the Supplier's delivery by:

Service Area	SLA description	Target
Supplier performance	Adherence to key milestones set out in Section 7 and the Statement of Work (SOW).	100% delivery before or on delivery milestone date.
Contract Management	Attendance at the monthly Contract Review meeting as described in section 17.	Monthly 100%
Contract Management	Monthly Update Note sent to the Contract Manager within 4 working days of a Monthly Contract Review Meeting	Monthly 100%
Invoicing/Billing	Compliant and fully transparent breakdown in costs and shall accurately reflect the services provided. Frequency: monthly in arrears	100%

Reporting	Management reporting to 100% accuracy submitted on time as detailed in section 8. Frequency: monthly	100%
Replacement of key personnel	Notification at the contract management review meeting with the contract manager.	TBA through contracting discussions.

Managing poor performance

Where the Contracting Authority identifies poor performance (3 consecutive agreed failures in any rolling 2-month period against agreed service delivery and SLAs, the Supplier shall be required to attend a performance review meeting to understand the issues and how to rectify them. The performance review meeting shall be at an agreed time no later than 5 working days from the date of notification. This may take place virtually or at the Contracting Authority's premises.

The Supplier shall be required to provide a full incident report which describes the issues and identifies the causes. The Supplier will also be required to prepare a full and robust 'Service Improvement Action Plan' which sets out its proposals

to remedy the service failure. The Service Improvement Plan will be subject to amendment following a performance review meeting and will be agreed by both parties prior to implementation.

The Contracting Authority will work with the Supplier to resolve any service failures; however, it will remain the Supplier's responsibility to resolve any/all service failure issues to ensure the service is delivered against the agreed milestones.

DEFINITIONS

Expression or Acronym	Definition
Contract	**Create a straightforward process to enable customers to define their requirements, search for a Commercial Agreement and then build a specification, to choose whether to direct award, compete or take the specification offline including where necessary the creation of a contract award notice.**
CA	**Commercial Agreement**
RFP	**request for price, or Invitation to Tender (ITT)**
Customers	**This can also mean Users and Buyers**

Supplier	**Delivery Partner**
DDS	**CCS Digital Services Directorate**
SOW	**Statement of Work**
BAU	**Business as Usual**
SRO	**Senior Responsible Officer**
CRM	**Customer Relationship Management**
ADR	**Architect Design Records**
E2E	**End to End**
EOI	**Express of Interest**
BPSS	**Baseline Personnel Security Standard**
GDS	**Government Digital Services is a professional body with which CCS will adhere to the assessment of and implement any government platforms. https://www.gov.uk/service-manual/service-standard**
Sprint	**It is expected that the Delivery Partner will work in fortnightly sprints, embedding agile best practice.**
User Interface	**User interfaces are the access points where users interact with designs**

SECURITY AND CONFIDENTIALITY REQUIREMENTS

A Non-Disclosure Agreement will need to be signed before the Contract Award.

Security clearance (BPSS) is required for the Supplier staff to receive access and work on Official Sensitive project information. The Supplier shall provide evidence that this is in place within the first 4 weeks of the contract.

Physical security checks will also be required to work or visit any of our CCS offices located in Liverpool, Newport, Bristol, Birmingham, Norwich and London. A CCS office-building pass will be granted, if required.

No Personal data shall be processed or stored on the Service Provider infrastructure without the explicit approval of the CCS Data Protection Manager. If approval is given to process personal data, the Supplier shall provide a Data Privacy Impact Assessment (DPIA) defining the privacy-related risk and controls be put in place to ensure it is appropriately protected.

All information released to the Supplier shall be treated as OFFICIAL and only stored and/ or processed in a manner throughout the contracted period where the security risk exposure is within the risk tolerance of the Contracting Authority and the Service Provider has obtained Cyber Essential certification.

The Supplier shall provide a Security Management Plan to be applied throughout the Design, Development and Deployment activities and shall submit to the Contracting Authority within the timescales defined therein.

All Contracting Authority OFFICIAL data provided in support of this agreement shall not be used for any other purpose than meeting the Contracting Authority's requirements under this Statement of Requirement. At the end of this contract, the Supplier shall provide evidence, to the satisfaction of the Contracting Authority, that it has securely deleted all OFFICIAL data in accordance with HMG guidance.

The Supplier shall make provision to provide IT equipment for each of their Team under this agreement. Where the Supplier is provisioned with Contracting Authority IT in support of this agreement, the Supplier shall ensure any individual who is provided with such equipment shall accept all the acceptable use policy. Any failure to comply shall be reported to the Contracting Authority and appropriate action taken to hold the individual accountable.

The Supplier shall nominate a single individual within their team to be accountable for all such provisioned Authority IT. If the Supplier detects a potential security incident, this shall be reported within 24 hours of detection.

ACCEPTANCE CRITERIA

(a) 15.1

PAYMENT AND INVOICING

Payment can only be made following satisfactory delivery of pre-agreed outcome phases, at the end of each stage prior to commencing the next stage of delivery.

A breakdown of work completed against the milestones in section 5 and associated costs should be submitted by the Supplier.

Payment and delivery will be managed by defined Statement of Works (SoWs) which shall be agreed with CCS and the Supplier**.**

Invoices will be submitted monthly in arrears. The Contracting Authority will pay the supplier within 30 days of receipt of the invoice.

Electronic Invoices should be submitted to the following email address for request for payment: supplierinvoices@crowncommercial.gov.uk

All submitted invoices should contain the Contract Reference, Purchase Order number and a full detailed breakdown of individual roles and aligned to the SOWs.

CONTRACT MANAGEMENT

Meetings between the Contracting Authority and Supplier will take place remotely (via agreed remote conferencing system) on a once a month basis as daily meetings with the Supplier will continue on operational delivery.

The Contracting Authority will provide the Supplier with details of their nominated Contract Manager(s) and Commercial Contract Manager(s) and relevant Deputies.

The Supplier's nominated personnel relevant to this agreement shall be required to attend the review meetings at the Contracting authority's premises and/or by conference calls/video conferencing, depending on COVID-19 pandemic restrictions in place, to assess and review but not limited to:

10.3.1 Adherence to SLAs – via review of submitted reports;

10.3.2 Issues and implementation of resolution plans;

10.3.3 Risk logs;

10.3.4 Agreement of Change Controls; and

10.3.5 Security management plan

10.3.6 Exit plan

10.4 Full details of the escalation process specifically relating to this contract are required, to include full contact details of senior representatives and issue resolution processes covering all aspects of service delivery as outlined within the Statement of Requirements, inclusive of out of hours' escalation points.

10.5 Supplier performance issues will be escalated to the Account Manager and shall be resolved within 5 working days of escalation.

10.6 The Supplier shall provide a dedicated Account Manager with a nominated Deputy who can act in their absence.

10.7 The Account Manager shall promote, deliver and communicate transparency of pricing, and savings to the Customer respectively.

10.8 Attendance at Contract Review meetings shall be at the Suppliers own expense if required to attend one of CCS's sites.

11. EXIT

11.3 The Supplier shall provide reasonable assistance to the Contracting Authority in order to assist the Contracting Authority in achieving the successful migration of the Provision (as the case may be) without undue delay or obstruction.

11.4 The Supplier shall provide the Contracting Authority with the exit plan within 1 month of contract mobilisation/inception meeting.

11.5 The Supplier shall present to the Contracting Authority any plans that may be required. This shall be agreed upon at the inception of the contract.

12. LOCATION

12.3 The location of the Services will be carried out at the offices of the Delivery Partner or CCS (Newport/ London/ Liverpool, Birmingham or remote working).

12.4 Near and Offshore - explore and provide details of Suppliers resources that are not staffing these should be provided in the bid to CCS.

12.5 These requirements indicate how to effectively deliver Scale for CCS, and the best environment. Exclusions for National Holidays will be agreed with CCS.

13. INTELLECTUAL PROPERTY RIGHTS (IPR)

13.3 Creation and ownership of IPR for Scale will be CCS proprietary owned.

13.4 No work delivered, developed, created or built that is related to the delivery of all requirements under any resultant Contract will have the IPR retained by the Supplier. All IPR will be transferred to CCS throughout the course of any resultant Contract.

13.5 The Supplier will advise on the optimal position for the Contracting Authority.

14. PROCUREMENT TRANSPARENCY

14.3 Please also note the Open contract standards which CCS must adhere to during the design of Scale https://www.gov.uk/government/publications/open standards-for-government/open-contractingdata-standard-profile

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the
Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

- **REDACTED TEXT under FOIA Section 43 Commercial Interests**.
- **REDACTED TEXT under FOIA Section 43 Commercial Interests**.

- Total £475,000

Invoice schedule

Milestone	Description	Acceptance criteria	Value	Expected Date
REDACTED TEXT under FOIA Section 43 Commercial Interests.	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**
REDACTED TEXT under FOIA Section 43 Commercial Interests.	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**
REDACTED TEXT under FOIA Section 43 Commercial Interests.	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**
REDACTED TEXT under FOIA Section 43 Commercial Interests.	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**	**REDACTED TEXT under FOIA Section 43 Commercial Interests.**

Schedule 7: UK GDPR Information

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

Annex 1: Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the
Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**.

1.2 The contact details of the Supplier's Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**.

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below **The Supplier is Controller and the Buyer is Processor**

	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 16 of the following Personal Data: • **N/A** **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: • **N/A** **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • *Business contact details of* Supplier Personnel for which the Supplier is the Controller, • *Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller,* • ***N/A***

Duration of the Processing	For the duration of the agreement Call Off Agreement
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this Framework Agreement including i. Ensuring effective communication between the Supplier and CSS ii. Maintaining full and accurate records of every Call-Off Contract arising under the Framework Agreement in accordance with Clause 7.6
Type of Personal Data	Includes: i. Contact details of, and communications with, CSS staff concerned with management of the Framework Agreement

	ii. Contact details of, and communications with, Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement, iii. Contact details, and communications with, Supplier staff concerned with fulfilment of the Supplier's obligations arising from this Framework Agreement Contact details, and communications with Supplier staff concerned with management of the Framework Agreement ii. Wider Public Sector research participants professional details including name, role, work email, work phone number.
Categories of Data Subject	Includes: i. CSS staff concerned with management of the Framework Agreement ii. Buyer staff concerned with award and management of Call Off Contracts awarded under the Framework Agreement iii. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Agreement

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All relevant data to be deleted 7 years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [**select: Supplier or Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as

Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**select: Supplier's or Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every [**insert number**] months on:

(i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful
disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their ’s duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete

at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal
Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the
Supplier's data security and privacy procedures relating to
Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the
Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body.
The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

8.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (Joint Controller Agreement), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

10.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable

after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection
Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.