

CQC

Provision of E Services for Disclosure Barring Services (DBS)

Ref: CQC CS 033

Call-Off Contract G-Cloud 14 Framework Agreement
(RM1557.14) Software and Support

LOT1: Cloud Hosting

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	733292166000655
Call-Off Contract reference	CQC CS 033
Call-Off Contract title	Provision of E Services for Disclosure Barring Services (DBS)
Call-Off Contract description	<p>To provide CQC with a full administration of the online applications process for disclosure and barring services checks as well as the essential requirement of a national ID checking service specifically designed for CQC staff.</p> <p>To include specific information relevant to the applicant's role in a drop-down format within the online application.</p> <p>CQC are also seeking access to the provision of advice on DBS policies and procedures, as laid down by the Disclosure and Barring Service.</p>
Start date	01/07/2025
Expiry date	30/06/2028
Call-Off Contract value	£133,760.00 Exc VAT £140,720.00 Inc VAT
Charging method	Electronic invoicing monthly
Purchase order number	To Be Provided

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14). Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

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

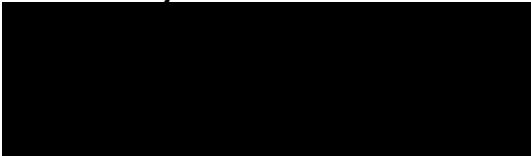
There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	Care Quality Commission Citygate, Gallowgate Newcastle upon Tyne NE1 4PA England
To the Supplier	Atlantic Data Ltd Atlantic House

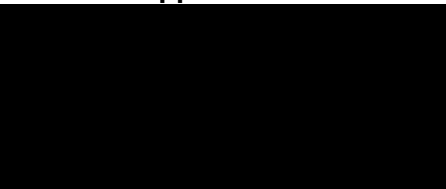
	7 Davy Avenue, Knowlhill, Milton Keynes, MK5 8HJ Company number: 04085856
Together the ‘Parties’	

Principal contact details

For the Buyer:



For the Supplier:



Call-Off Contract term

Start date	This Call-Off Contract Starts on 01st July 2025 and is valid for 36 Months .
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>
Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 1 Month's written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>

Buyer contractual details

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

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 2: Cloud Software
G-Cloud Services required	<ul style="list-style-type: none"> • To provide CQC with a full administration of on-line applications for disclosure and barring services checks as well as the essential requirement of a national ID checking service specifically designed for CQC staff • This needs to include specific information relevant to the applicant's role, in a drop-down format within the online application and should include CQC specific information such as Job Role, Location, and Directorate. • In addition, CQC are also seeking access to the provision of advice on DBS policies and procedures, as laid down by the Disclosure and Barring Service. • As part of the service provision, CQC will require both the user DBS applicant and Human Resources to have full access to a CQC branded site to enable us to send and monitor applications, as well as access to a full management information reporting function to enable us to manage ongoing applications, verify and track all applications within the checking process including initial confirmation confirming if a check is clear or contains information. • CQC must therefore be able to access this information in-house and online.
Additional Services	NOT USED
Location	The Services will be Online remote delivery
Quality Standards	The Supplier is required to deliver the Services under this agreement according to best industry practice. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to deliver a quality service consistently. See Annex 1 & 1a
Technical Standards:	The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

	The Supplier shall deliver the contract requirements securely and in compliance with Disclosure and Barring Service procedures. They shall have fully developed and tested business continuity and disaster recovery plans for the system and premises.
Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are</p> <ul style="list-style-type: none"> • Atlantic Data makes a service level commitment to its clients which guarantees that its online and support services will be available to users between 9am and 5pm. • In practice though, the online aspects of the Disclosures system are available 24 hours a day 7 days a week. • Disclosures users benefit from a system which boasts in excess of 99% uptime.
Onboarding	<p>The onboarding plan for this Call-Off Contract is</p> <ul style="list-style-type: none"> • No Onboarding Plan is required as the Supplier is the incumbent Supplier.
Offboarding	<p>The offboarding plan for this Call-Off Contract is</p> <ul style="list-style-type: none"> • The Supplier is required to ensure the orderly transition of the Service from the Supplier to the Buyer and/or Replacement Supplier in the event of termination or expiry of Call Off Contract. • Supplier to provide exit strategy within 90 days of the Contract start date.
Collaboration agreement	NOT USED
Limit on Parties' liability	<ul style="list-style-type: none"> • The annual total liability of either Party for all Property Defaults will not exceed 125% of the contract value. • The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. • The annual total liability for all other Defaults will not exceed the greater 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater


Buyer's responsibilities	<p>The Buyer is responsible for:</p> <ul style="list-style-type: none"> Nominate a lead within the organisation to oversee the delivery of the service from an internal perspective and to report ad hoc issues, requests and amendments, as required, attend meetings with the Supplier (to be determined) and to review the service and ensure it remains compliant with CQC's requirements. CQC's HR Team will be responsible for sending all invites to staff who are required to complete a DBS check and will monitor the E service through the supplier's portal to ensure staff compliance. CQC will run monthly reports to verify applications that have been processed through the portal and to check on average time frames from invitation to result received.
Buyer's equipment	NOT USED

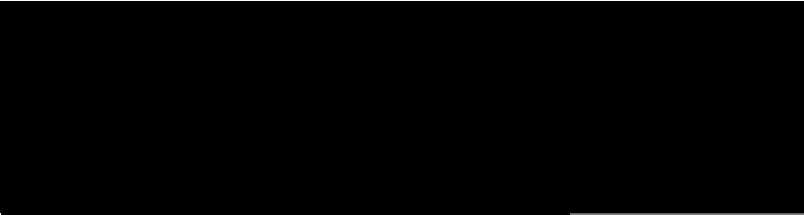
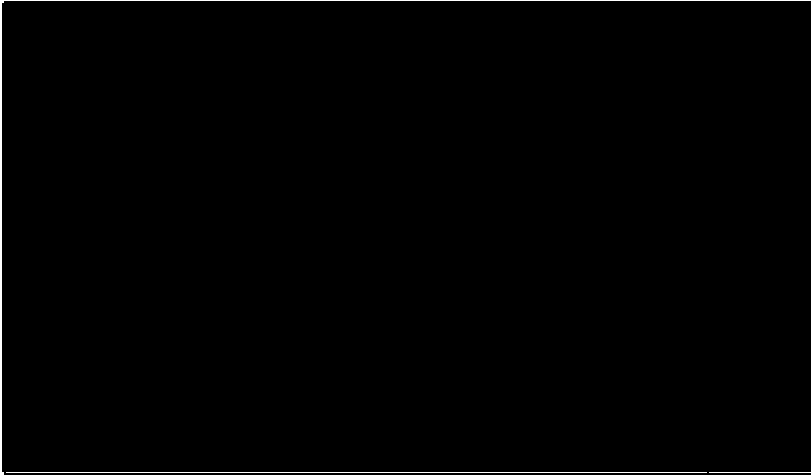
Supplier's information

Subcontractors or partners	NOT USED
-----------------------------------	-----------------

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 BACS.
Payment profile	The payment profile for this Call-Off Contract is monthly
Invoice details	The Supplier will issue electronic invoices monthly . The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	
Invoice information required	All invoices must include a valid purchase order number and be sent to the above email address to enable payment.

Invoice frequency	The invoice will be sent to the Buyer Monthly.
Call-Off Contract value	The total value of this Call-Off Contract is up to £133,760.00 Exc VAT £140,720.00 Inc VAT.
Call-Off Contract charges	<p>The breakdown of the Charges is</p> <ol style="list-style-type: none">Post Office ID checking<ul style="list-style-type: none">Admin fees payable by the applicant via the Post Office.CQC-specific job roles.CQC branding.The charges for the CQC service are as follows: In addition, there are the DBS and Post Office ID check fees as follows:  <p>All fees are exclusive of VAT which is charged at the prevailing rate. The DBS fee is VAT-exempt.</p>

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none"> • Supplier to provide exit strategy. • Copy of Business Disaster Recovery Plan. • Copy of Business Continuity Plan
Guarantee	NOT USED
Warranties, representations	NOT USED
Supplemental requirements in addition to the Call-Off terms	NOT USED
Alternative clauses	NOT USED
Buyer specific amendments to/refinements of the Call-Off Contract terms	NOT USED
Personal Data and Data Subjects	Annex 1 of Schedule 7 applies.
Social Value	Below Threshold
Performance Indicators	<p>Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.</p> <p>Note required Performance Indicators needed from the Supplier for future publication.</p>

1. Formation of contract

- 1.1. By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2. The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3. This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4. In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive of the Framework Agreement.

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

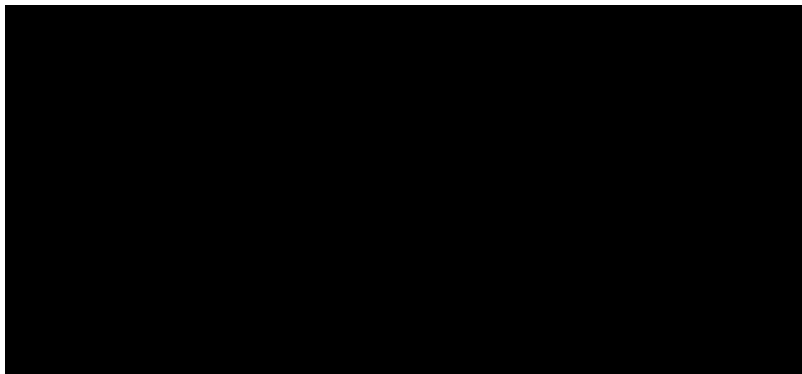
Buyer Benefits

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

[G-Cloud 14 Customer Benefit Record](#)

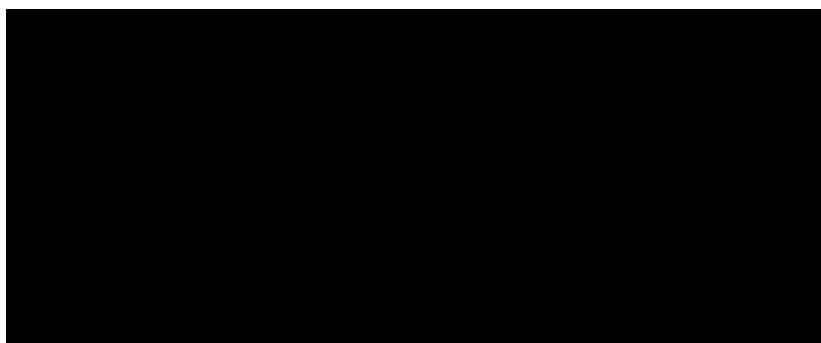
IN WITNESS of which this Contract has been duly executed by the parties.
SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:



SIGNED for and on behalf of **Atlantic Data Ltd**

Authorised Signatory 1:



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.
- 1.3. 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.
- 1.4. 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.
- 1.5. The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 36 months

2. Incorporation of terms

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 30 (Insurance)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)

- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

- 2.2.1. a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- 2.2.2. a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
- 2.2.3. a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

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

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

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

3. Supply of services

- 3.1. The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2. The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form

4. Supplier staff

4.1. The Supplier Staff must:

- 4.1.1. be appropriately experienced, qualified and trained to supply the Services.
- 4.1.2. apply all due skill, care and diligence in faithfully performing those duties.
- 4.1.3. obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer.
- 4.1.4. respond to any enquiries about the Services as soon as reasonably possible.
- 4.1.5. complete any necessary Supplier Staff vetting as specified by the Buyer.

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

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

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

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

- 4.6. The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7. If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8. If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

- 5.1. Both Parties agree that when entering into a Call-Off Contract they:
 - 5.1.1. have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party.
 - 5.1.2. are confident that they can fulfil their obligations according to the Call-Off Contract terms.
 - 5.1.3. have raised all due diligence questions before signing the Call-Off Contract.
 - 5.1.4. have entered into the Call-Off Contract relying on their own due diligence.

6. Business continuity and disaster recovery

- 6.1. The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.
- 6.2. The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3. If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

- 7.1. The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2. The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3. The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4. If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5. The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

- 7.6. If the Supplier enters into a Subcontract, it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7. All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8. The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9. The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10. The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11. If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does, then the Supplier must provide a replacement valid invoice with the response.
- 7.12. Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1. The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2. The Supplier will ensure that:
 - 9.2.1. during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000.
 - 9.2.2. the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit.
 - 9.2.3. all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date.
 - 9.2.4. all agents and professional consultants involved in the Services hold employers' liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date.

- 9.3. If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4. If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
 - 9.4.1. a broker's verification of insurance.
 - 9.4.2. receipts for the insurance premium.
 - 9.4.3. evidence of payment of the latest premiums due.
- 9.5. Insurance will not relieve the Supplier of any liabilities under the Framework Agreement, or this Call-Off Contract and the Supplier will:
 - 9.5.1. take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers.
 - 9.5.2. promptly notify the insurers in writing of any relevant material fact under any Insurances.
 - 9.5.3. hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance.

10. Confidentiality

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

11. Intellectual Property Rights

- 11.1. Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2. Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.
- 11.3. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:
 - 11.3.1. any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and
 - 11.3.2. The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

- 11.4 . The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.
- 11.5. Subject to the limitation in Clause 24.3, the Buyer shall:
- 11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
- a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
 - b) alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;
 - c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and
- 11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.
- 11.6. The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
- 11.6.1. rights granted to the Buyer under this Call-Off Contract.
- 11.6.2. Supplier's performance of the Services.
- 11.6.3. use by the Buyer of the Services
- 11.7. If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
- 11.7.1. modify the relevant part of the Services without reducing its functionality or performance.
- 11.7.2. substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer.
- 11.7.3. buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer.
- 11.8. Clause 11.6 will not apply if the IPR Claim is from:
- 11.8.1. the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
- 11.8.2. other material provided by the Buyer necessary for the Services
- 11.9. If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1. The Supplier must:

- 12.1.1. comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data
- 12.1.2. only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- 12.1.3. take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

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

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

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

13. Buyer data

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

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

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: [Security policy framework: protecting government assets - GOV.UK](#)
- 13.6.2 the Government Security - Classification policy: [Government Security Classifications - GOV.UK](#)
- 13.6.3 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: [Adopt a Risk Management Approach | Passport to Good Security | NPSA](#)

- 13.6.4 and Protection of Sensitive Information and Assets: [Sensitive Information & Assets | System & Information Security | NPSA](#)
 - 13.6.5 the National Cyber Security Centre's (NCSC) information risk management guidance: [Risk management - NCSC.GOV.UK](#)
 - 13.6.6 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: [The Technology Code of Practice - GOV.UK](#)
 - 13.6.7 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: [The cloud security principles - NCSC.GOV.UK](#)
 - 13.6.8 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: [The Technology Code of Practice - GOV.UK](#)
- 14.3. If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4. If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5. The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security, and the Supplier agrees that the

Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

16. Security

- 16.1. If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2. The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3. If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4. Responsibility for costs will be at the:
 - 16.4.1. Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided.
 - 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control.
- 16.5. The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6. Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance: [10 Steps to Cyber Security - NCSC.GOV.UK](https://www.ncsc.gov.uk/10-steps-to-cyber-security)
- 16.7. If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

- 17.1. If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:
 - 17.1.1. an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

- 18.1. The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.
- 18.2. The Parties agree that the:
- 18.2.1. Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
 - 18.2.2. Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses
- 18.3. Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4. The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
- 18.4.1. a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
 - 18.4.2. any fraud
- 18.5. A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
- 18.5.1. the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
 - 18.5.2. an Insolvency Event of the other Party happens
 - 18.5.3. the other Party ceases or threatens to cease to carry on the whole or any material part of its business
- 18.6. If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
- 18.7. A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

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

- 19.2. Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.
- 19.3. The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4. Ending or expiry of this Call-Off Contract will not affect:
- 19.4.1 any rights, remedies or obligations accrued before its Ending or expiration
 - 19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry
 - 19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
 - 7 (Payment, VAT and Call-Off Contract charges)
 - 8 (Recovery of sums due and right of set-off)
 - 9 (Insurance)
 - 10 (Confidentiality)
 - 11 (Intellectual property rights)
 - 12 (Protection of information)
 - 13 (Buyer data)
 - 19 (Consequences of suspension, ending and expiry)
 - 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)
 - 19.4.4 Any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.
- 19.5. At the end of the Call-Off Contract Term, the Supplier must promptly:
- 19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
 - 19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
 - 19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
 - 19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
 - 19.5.5 work with the Buyer on any ongoing work
 - 19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
- 19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

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

- 21.6.1. the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
- 21.6.2. there will be no adverse impact on service continuity.
- 21.6.3. there is no vendor lock-in to the Supplier's Service at exit.
- 21.6.4. it enables the Buyer to meet its obligations under the Technology Code of Practice.

- 21.7. If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8. The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
- 21.8.1. the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - 21.8.2. the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
 - 21.8.3. the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
 - 21.8.4. the testing and assurance strategy for exported Buyer Data
 - 21.8.5. if relevant, TUPE-related activity to comply with the TUPE regulations
 - 21.8.6. any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition.

22. Handover to replacement supplier

- 22.1. At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
- 22.1.1. data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
 - 22.1.2. other information reasonably requested by the Buyer
- 22.2. On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.
- 22.3. This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

- 23.1. Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.
- 23.2. A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3. Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

24. Liability

- 24.1. Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).
- 24.2. Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:
- 24.2.1. pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and
 - 24.2.2. in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.
- 24.3. Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).
- 24.4. When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2. will not be taken into consideration.

25. Premises

- 25.1. If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2. The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3. The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4. This clause does not create a tenancy or exclusive right of occupation.
- 25.5. While on the Buyer's premises, the Supplier will:
- 25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises
 - 25.5.2 comply with Buyer requirements for the conduct of personnel
 - 25.5.3 comply with any health and safety measures implemented by the Buyer
 - 25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

- 26.1. The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.
- 26.2. Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.
- 26.3. When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

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

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

28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
 - 29.2.2 age
 - 29.2.3 start date
 - 29.2.4 place of work
 - 29.2.5 notice period
 - 29.2.6 redundancy payment entitlement
 - 29.2.7 salary, benefits and pension entitlements
 - 29.2.8 employment status
 - 29.2.9 identity of employer
 - 29.2.10 working arrangements
 - 29.2.11 outstanding liabilities
 - 29.2.12 sickness absence
 - 29.2.13 copies of all relevant employment contracts and related documents
 - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will cooperate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
- 29.6.1 its failure to comply with the provisions of this clause
 - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.3 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.4 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause, but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
- 31.2.1 work proactively and in good faith with each of the Buyer's contractors

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

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 if it isn't a material change to the Framework Agreement or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request using the template in Schedule 9. This includes any changes in the Supplier's supply chain.
- 32.3 If either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation or End this Call-Off Contract by giving 30 days' notice to the Supplier.

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services

Supplier Service Provision

Service Provision for the Care Quality Commission (CQC)
Provision of the Disclosures Manager System by Atlantic Data Ltd

Atlantic Data Ltd is pleased to offer the continued provision of its industry-leading Disclosures Manager system to support the Care Quality Commission (CQC) in fulfilling its statutory and organisational responsibilities regarding criminal records checking.

This proposal outlines how the Disclosures Manager solution—already deployed by CQC— will continue to provide secure, efficient, and fully configurable services to meet the specific needs of both the CQC’s HR department and any future expansion to include the National Contact Services Centre (NCSC).

1. **Comprehensive Criminal Records Checking Platform**
Disclosures Manager is a web-based software platform designed to streamline the processing and management of Disclosure and Barring Service (DBS) checks. Accessible via any internet-enabled device, the system provides 24/7 secure access for applicants and administrative users.

2. **CQC-Specific Configuration and Customisation**
Disclosures Manager is fully tailored to reflect CQC’s internal structures and compliance requirements. Key configuration elements include:

- Job role-specific parameters such as check level, workforce, volunteer/home-based status
- User hierarchies aligned to department, location, and directorate
- Pre-configured workflows to match CQC’s operational procedures

This ensures an optimised user experience and administrative efficiency for all DBS-related processes.

3. **CQC-Branded User Interface**
The CQC platform is custom branded with the organisation’s logo and visual identity, reinforcing familiarity and trust among applicants and internal users. Beyond white-labelling, Atlantic Data delivers a bespoke interface that supports CQC’s communications and brand consistency.

4. **Built-In Policy Guidance and Knowledge Resources**
A dedicated knowledgebase is available within the platform, offering:

- General guidance on DBS policies and procedures
- CQC-specific content, such as the policy on the recruitment of ex-offenders
- Configurable content management features to enable CQC to publish targeted guidance for users

This empowers CQC administrators and applicants with instant access to essential information.

5. **Intelligent Application Tracking and Reporting**
The Disclosures Manager system includes sophisticated monitoring and reporting tools:

- Real-time tracking of all applications via direct integration with the DBS system

- Automated alerts for stalled or delayed applications
- A suite of over 10 live management reports updated automatically
- Complete audit trails for compliance assurance

These tools enable the CQC to monitor progress, identify issues, and maintain high levels of process visibility and control.

6. Immediate Certificate Notifications

System users receive instant updates when a certificate is issued by the DBS. As soon as results are available, CQC users can view whether the certificate is clear or contains relevant information, facilitating timely decision-making and action.

7. Registered DBS Umbrella Body Services

Atlantic Data is a registered DBS Umbrella Body and e-Broker, authorised to process criminal records checks on behalf of organisations not directly registered with the DBS. This registration supports a compliant and streamlined service for the CQC.

8. Identity Verification Services – Digital ID

In alignment with evolving DBS guidance and digital transformation initiatives, Atlantic Data proposes the use of Digital ID verification as the default identity checking method. This secure and efficient solution allows applicants to verify their identity remotely using compliant digital credentials.

To ensure inclusivity and continuity, the existing arrangement for in-person or alternative ID verification methods will remain available as contingency options, enabling full compliance in cases where Digital ID cannot be used. The contingency options will be, Post Office IBV, Virtual ID with Posted Identity Docs and then Virtual ID Online Identity Docs.

9. Extension to NCSC Service Requirements

Atlantic Data is prepared to extend its services to support the CQC's National Contact Services Centre (NCSC) for processing DBS checks relating to care managers applying for registration. Given our existing role as supplier to both the HR and NCSC departments, we are uniquely positioned to deliver a unified and scalable solution, subject to further clarification of requirements.

Our experience delivering dual-service models is well-established across a range of sectors, including:

- University clients managing checks for both students and staff
- NHS Trusts supporting both direct employees and third-party health workers
- Legal sector clients managing checks for professionals and internal staff

10. Data Security and Compliance

Atlantic Data upholds the highest standards of data protection and operational security, including:

- Full ISO 27001 certification for information security
- Registration as a DBS e-Bulk provider
- Compliance with the Data Protection Act and GDPR
- Clear, documented procedures for incident management and reporting
- Availability of process lifecycle maps for annual review by the CQC

11. Business Continuity and Disaster Recovery

Disclosures Manager is supported by fully documented and tested Business Continuity Plans (BCP) and Disaster Recovery (DR) procedures, compliant with ISO 27001 and ISO

22301 standards. These plans ensure minimal disruption to services and fast recovery in the event of any system failure or external disruption.

12. High Availability and Support

Atlantic Data ensures exceptional system availability and client support:

- Regular maintenance scheduled between 12:00 a.m. and 6:00 a.m.
- Minimum two working days' notice for any planned outages outside this window
- Guaranteed downtime of less than 24 hours per rolling three-month period
- Dedicated Account Manager and access to a Client Support Team available weekdays from 9:00 a.m. to 5:00 p.m.

13. Responsiveness to Legislative and Procedural Change

Atlantic Data maintains close relationships with the DBS and the Criminal Records Trade Body, ensuring we remain at the forefront of procedural changes and innovations. Any new identity verification legislation or technical updates introduced by the Home Office or DBS will be promptly reviewed and, where applicable, incorporated into the service provided to the CQC.

Conclusion

Atlantic Data Ltd is proud to continue its partnership with the CQC, delivering a dependable, modern, and compliant criminal record checking system through Disclosures Manager. Our service ensures continued excellence, scalability, and flexibility to support the CQC's operational requirements, now and into the future.

We look forward to the opportunity to support both current and future aspects of the CQC's DBS checking responsibilities with innovation, responsiveness, and unwavering compliance.

Service Scope

Software add-on or extension	Yes, but can standalone
What software services is the service an extension to	Digital Identity and Right-to-Work services Other Background Screening Services
Cloud deployment model	Private
Service constraints	None
System requirements	<ul style="list-style-type: none"> • Disclosures is accessible via any internet-enabled PC or device. • There are no other system requirements for users.

User Support

Email or online ticketing support	Yes
Support response times	Questions can be submitted via telephone, email or a built-in secure messaging facility. An initial response to e-mails and messages is provided same working day. If the matter cannot be dealt with on the first contact, a priority approach is adopted whereby the most critical of technical issues are dealt with as a high priority. The majority of queries relate to DBS processes such as new applicant data not matching previous application data held on record by the DBS
User can manage status and priority of support tickets	Yes
Online ticketing support accessibility	Wcag aa
Phone support	Yes
Phone support availability	9 to 5 Mon to Fri
Web chat support	Yes, extra cost
Web chat support availability	9 to 5 Mon to Fri
Web chat support accessibility standard	Wcag aa
Onsite support	No
Support levels	Support for users of the Disclosures system is via a helpdesk and/or client relationship management team. Both of these support services are available 9am to 5pm. Each of these teams offer a level of technical support and are able to resolve the vast majority of technical issues. Specialist technical support is available via a priority-based ticketing system, which

	the helpdesk support advisers and relationship management team have access to. Key customers and customised accounts qualify for a dedicated account manager as primary contact for support. These customers are provided a unique email address and contact point. Support is included in annual account maintenance fees.
Support available to third parties	No

Onboarding and offboarding

Getting started	Client User On-boarding is a pre-planned phase within all new client user startups or launches. Disclosures and Disclosures Manager is intuitive and is provided with short 3 step training and initiation program of videos. Onsite training is available. The service Quick Start Guide and video tutorials have proved highly successful and meet most organisations training requirements. The Quick Start Guide is an online training module which takes users through the key functions of the system upon registration. Video tutorials provide more in-depth training on how to use key functionality within the system. An additional Inline help service is available to users throughout the Disclosures system. This aspect provides additional support to users about important key considerations such as name history or middle names.
Service documentation	Yes
Documentation formats	<ul style="list-style-type: none"> • HTML • PDF
End-of-contract data extraction	Certain Disclosures reports allows users to extract data at the end of the contract using the API feature. Otherwise, this can be managed by Atlantic Data on behalf of its customers.
End-of-contract process	The off-boarding process is largely straightforward. Atlantic Data will work with the organisation to establish a project requirement and timetable to agree any required actions as part of the transition. If a clients require Atlantic Data to consult or liaise with a new supplier at the end of the contract period, its reasonable costs of doing so would also be agreed with the customer in advance

Using the service

Web browser interface	Yes
Supported browsers	<ul style="list-style-type: none"> • IE11 • EDGE • FIREFOX • CHROME • SAFARI • OPERA
Application to install	No
Designed for use on mobile devices	Yes
Differences between the mobile and desktop service	Disclosures works on mobile devices with no difference in functionality.
Service interface	Yes
Description of service interface	Disclosures is accessible using an internet connection. Authorised users use their login credential together with Dual Factor Authentication security. Senior Client Administrators are able to set Access role rights and permissions i.e. initiating new DBS checks, I.D. check, to access management information and reports relevant to their area of responsibility.
Accessibility standards	Wcag_aa
Accessibility testing	One of Atlantic Data's key clients is a national disability charity, providing support and services to blind and partially sighted people across the UK, through the provision of guide dogs, mobility and other rehabilitation services. This national charity provided vital assistance to oversee Disclosures' WCAG2.1AA compliance, and by testing against assistive technologies, such as JAWS Screen Reader and Zoom Text Screen Magnification software.
API	Yes
What users can and can't do using the API	Disclosures offers API Integration. The API allows users to carry out a range of activities with 3rd party systems e.g.: - initiating a DBS application invitation - updating shared information - DBS application status information - cancellation applications Atlantic Data is also able to deliver alternative integration solutions, using most technical methods - SFTPS, SQL access and SOAP and REST API's.
API documentation	Yes
API documentation formats	pdf

API sandbox or test environment	Yes
Customisation available	Yes
Description of customisation	Refer to the Disclosures Manager service, which can be configured to suit the customers' requirements. Customisable aspects are varied but include: - job role descriptions specific to the organisation's requirements - combinations and levels of DBS checks to suit the customer's needs - users configured within a structure of departments, branches and divisions to reflect the customer's own corporate structure, or physical network of offices. - an application/information flow which suits the customer's own business processes - a variety of I.D. check options, including outsourcing to 3rd parties, such as the Post Office - tailored reports and export data, such as financial information - corporate branding - integration with customers' own/third party systems

Scaling

Independence of resources	Atlantic Data is an IT services organisation with a full technical and IT capability. Atlantic Data supports its own IT server network and infrastructure with a full DR capability. Each client is maintained on their own dedicated virtual instance within Atlantic's cloud service. using Tier one connectivity Atlantic has a proven record on 99% uptime. Dynamic load and resource management enables our IT division to maintain a highly scalable resource centre. This level of infrastructure enables clients and service users to receive consistent high levels of service accessibly.
---------------------------	---

Analytics

Infrastructure or service metrics	Yes
Metrics types	Disclosures has a suite of management reports which allow users to track applications, as well as obtain useful M.I. regarding the organisation's Disclosure applications.
Reporting types	<ul style="list-style-type: none"> • API • REAL-TIME • REGULAR-REPORTS • ON-REQUEST

Resellers

Supplier type	Not reseller
---------------	--------------

Staff security

Staff security clearance	STAFF SCREENING NOT BS7858 2019
Government security clearance	DV

Asset protection

Knowledge of data storage and processing locations	Yes
Data storage and processing locations	UK
User control over data storage and processing locations	No
Penetration testing frequency	At least once a year
Protecting data at rest	<ul style="list-style-type: none"> • Csa ccm • Encrypted media • Scale obfuscation sharding
Data sanitisation process	Yes
Data sanitisation type	<ul style="list-style-type: none"> • Overwriting • No access
Equipment disposal approach	Recognised standard

Data importing and exporting

Data export approach	The export of data can be achieved in a number of ways. Typically, through an API . Bespoke versions of Disclosures contain a customised export facility with fields of data specifically agreed with the customer. Otherwise, this can be managed by Atlantic Data on behalf of its customers. Otherwise, this can be managed by Atlantic Data on behalf of its customers.
Data export formats	<ul style="list-style-type: none"> • CSV
Data import formats	<ul style="list-style-type: none"> • CSV

Data-in-transit protection

Data protection between buyer and supplier networks	<ul style="list-style-type: none"> • PRIVATE OR PSN • TLS • LEGACY SSL
Data protection within supplier network	<ul style="list-style-type: none"> • TLS

Availability and resilience

Guaranteed availability	Atlantic Data makes a service level commitment to its clients which guarantees that its online and support services will be available to users between 9am and 5pm. In practice though, the online aspects of the Disclosures system are available 24 hours a day 7 days a week. Disclosures users benefit from a system which boasts in excess of 99% uptime.
Approach to resilience	As an ISO 27001-certified organisation for IT security management systems, Atlantic Data implements robust measures to ensure resilience. Such measures include SLAs, disaster recovery and business continuity planning, and historic performance demonstrates an uptime in excess of 99%. Further information about the resilience of Atlantic Data's systems are available on request. Further information about the resilience of Atlantic Data's systems are available on request.
Outage reporting	Atlantic Data maintains a log management service policy. As a part of internal framework authorised systems administrators review the audit trail logs daily. These logs capture and store reports in a centralised log analyser, which proactively triggers alerts on suspicious activity and authentication failures. Root cause analysis processes and procedures address potential security threats and incidents that may occur and appropriate corrective action is taken to address and prevent further occurrences. Where necessary, outages are reported to affected customers via a combination of system messages, public dashboard, email alerts and personal client relationship contact.

Identity and authentication

User authentication needed	Yes
User authentication	<ul style="list-style-type: none"> • TWO FACTORS • PKA • DEDICATED LINK • USERNAME OR PASSWORD

Access restrictions in management interfaces and support channels	Atlantic Data maintains an access control policy, which details the segregation of duties and ensures the confidentiality and integrity of data by restricting access only to authorised personnel. User access is granted only after a formal authorisation process. Most Disclosures systems adopt a role-based access principle. All access is provided by creating unique user credentials which helps in audit trails. The service is configured with multiple levels of privileges based on the roles, which ensures the confidentiality of the data by segregation of duties. Support services are provided by utilising registered user passwords.
Access restriction testing frequency	At least once a year
Management access authentication	<ul style="list-style-type: none"> • Two factors • Public key • Dedicated link • Username or password

Audit information for users

Access to user activity audit information	Real time
How long user audit data is stored for	At least 12 months
Access to supplier activity audit information	Real time
How long supplier audit data is stored for	Over 12 months
How long system logs are stored for	At least 12 months

Standards and certifications

ISO/IEC 27001 certification	Yes
Who accredited the ISO/IEC 27001	British Standards Institution
ISO/IEC 27001 accreditation date	28/01/2022 (01/02/2007 was the original accreditation)
What the ISO/IEC 27001 doesn't cover	The certification covers business process outsourcing services, software development and support, client administration, customer support, DBS umbrella body services, compliance with UK data protection legislation, eBulk services, hosting and web services, support functions such as legal, IT, administration and facilities.

ISO 28000:2007 certification	No
CSA STAR certification	No
PCI certification	Yes
Who accredited the PCI DSS certification	Self-certificated
PCI DSS accreditation date	3 April 2020
What the PCI DSS doesn't cover	Current Attestation is for PCI level 4
Other security certifications	Yes
Any other security certifications	ISO 27001

Security governance

Named board-level person responsible for service security	Yes
Security governance certified	Yes
Security governance standards	ISO IEC 27001
Information security policies and processes	Atlantic Data is ISO 27001-certified. Some of the security measures in place are as follows:- clear desk and clear screen policy, restricted physical access within the premises to authorised personnel, shred/disposal of sensitive data policies, password policy, physical and environmental controls (e.g. biometric access doors and RFID), encryption of data in transit and at rest, firewall policy, visitor management processes and an annual IT health check. In addition to the above, Atlantic Data has an internal security forum, with representation at board level, to review regular updates on security on a periodic basis and monitor compliance with policies and process. Compliance with policies and processes is also ensured through rigorous training, internal and external audits.

Operational security

Configuration and change management standard	Recognised standard
--	---------------------

Configuration and change management approach	Changes to Atlantic Data's Disclosures systems invariably stem from one of three main sources 1. Changes initiated by a change in process by the DBS. 2. Changes requested by the client. 3. Changes/modifications/upgrades to the system initiated by Atlantic Data. In any of these cases, Atlantic Data follows a strict change management process as part of its ISO 27001 controls. This includes robust tracking and monitoring of all change requests. Before being deployed to a live environment, any changes are tested in a staging environment for QA and assessed for risks, such as any potential impact on security.
Vulnerability management type	Recognised standard
Vulnerability management approach	Atlantic Data has an Internal Security Forum which regularly reviews updates on security. All systems and the environments they are hosted on are regularly reviewed. Independent IT health checks are conducted, and appropriate fixes are applied. The workstation environment is also patched regularly to address vulnerabilities. The IT perimeter is secured using the EAL4+-compliant UTM which acts as the IPS system. The production systems are configured using iptables, firewall, TCP wrappers and application firewalls. All these systems report to a centralised log analyser, which records an audit trail of any incident and triggers alerts on suspicious activity to authorised personnel.
Protective monitoring type	Recognised standard
Protective monitoring approach	Atlantic Data carries out protective monitoring via a centralised log analyser. This allows authorised systems administrators to review logs on a daily basis. The analyser proactively triggers alerts on any suspicious activity or authentication failures. A root cause analysis process ensures that in the event of any security incidents appropriate and timely corrective action is taken to correct that instance and prevent any future occurrence. Incidents are addressed immediately.
Incident management type	Recognised standard
Incident management approach	Atlantic Data's disaster recovery plan and business continuity plans define the processes necessary for the effective restoration/recovery of critical functions. The plans detail strategies for business recovery, plans in the event of communication failure, testing, key employee contact lists, and vendors' emergency contacts. The RTO for IT infrastructure, data and client support is 24 hours. A back-up site is isolated from Atlantic Data's primary location on a TIER 4 datacentre with the same level of security controls and resilience as the primary. The DR site is a mirror of the production set up and capable of the shortest of RPO.

Secure development

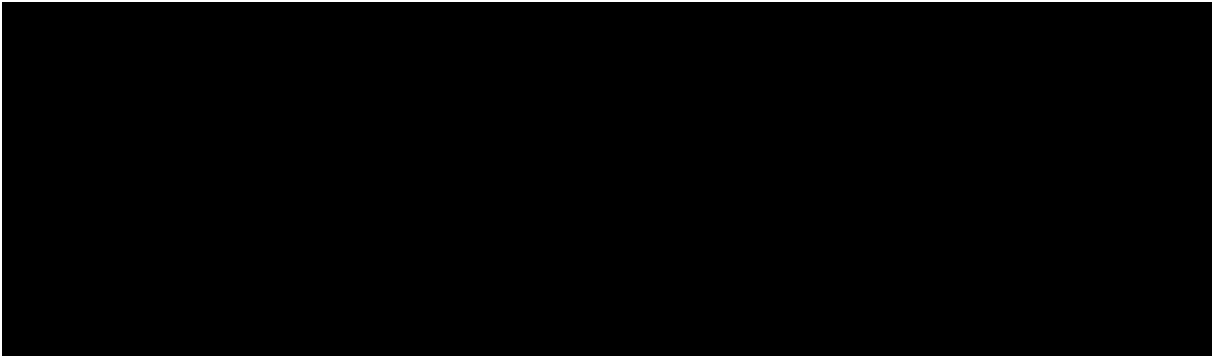
Approach to secure software development best practice	Independent review
---	--------------------

Public sector networks

Connection to public sector networks	Yes
Connected networks	Yes
Other public sector networks	<ul style="list-style-type: none">• The Disclosures and Barring Service's e-Bulk network• CJSM

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:



Description	Cost (Excluding VAT)	Frequency of Payment

Service summary:

Quotation for the contract renewal of the DBS Umbrella Service, with ADL acting as the Registered Body. The application software will be Disclosures Manager (V3) with the additional of Digital Identity, Virtual Identity and Card Payment modules.

Based on the discussions, the volumes have been set at [REDACTED]. Volumes will be reviewed by the Account Manager throughout the year with adjustments made where necessary.

Pricing is based upon CQC HR paying for DBS fees, Route 2 and missed video call fees and applicants paying for the identity and admin fee.

The prices quoted for the admin fee and Maintenance fee will [REDACTED] year on year.

All prices quoted exclude VAT. VAT does not apply to the DBS Fee.

Identity Check Options

The default identity checking methodology will be Digital Identity. This process will be

implemented within the CQC HR service when the contract renews.

As a requirement of DBS guidelines there are three contingency identity checking methods built into the Disclosures Manager service. These will be offered to applicants where they are unable, or unwilling, to undertake a Digital Identity check. They will be offered in the order given below

ID Check Contingency 1 – Post Office

Applicant selects their documents in the application then attends the Post Office for a Face-to-Face document check.

ID Check Contingency 2 – Postal Virtual

Applicant posts their identity documents to Atlantic Data and this validated prior to a video call with the applicant.

ID Check Contingency 3 – Online Virtual

Applicant uploads images of their identity documents to the application prior to a video call.

Pricing includes the implementation of a card payment service for the admin fee and Digital ID (or Virtual ID) – DBS fees will not be collected from the applicant.

Please note:

Development may not be delivered until payment is received.

Cost has been calculated based on the known scope of the project as detailed in this quotation.

All other previously agreed fees remain the same.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form, set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	a) the UK GDPR as amended from time to time; b) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; c) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	Default is any: <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE').
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.

Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
------------------	---

ESI Reference Number	The 14-digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	The following financial and accounting measures: <ul style="list-style-type: none"> • Dun and Bradstreet score of 50 • Operating Profit Margin of 2% • Net Worth of 0 • Quick Ratio of 0.7

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available • The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force • Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	<p>A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.14 together with the Framework Schedules.</p>
Fraud	<p>Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.</p>
Freedom of Information Act or FoIA	<p>The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or</p>

	codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

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

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity <ul style="list-style-type: none"> ○ commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.

Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.

Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see Spend controls: check if you need approval to spend money on a service - Service Manual - GOV.UK
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.

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

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]
- 1.2 The contact details of the Supplier's Data Protection Officer are [REDACTED] email [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	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, the Buyer is the Controller, and the Supplier is the Processor of the following Personal Data: <ul style="list-style-type: none"> • Name and contact details. • Date of Birth. • National Insurance Number. • Job Title. • Disclosure reference number. • Confirmation if an application holds information regarding a criminal conviction
Duration of the Processing	From the start of the contract (01/07/2025) until the end of this contract (30/06/2028) and any agreed extension period thereafter (up to 30/06/2029).
Nature and purposes of the Processing	To enable CQC to apply and process DBS checks for new staff and refresh for existing staff.
Type of Personal Data	Data required to complete a DBS application · Name and contact details <ul style="list-style-type: none"> • Date of Birth. • National Insurance Number. • Job Title · Disclosure reference number. • Confirmation if an application holds information regarding a criminal conviction
Categories of Data Subject	<ul style="list-style-type: none"> • CQC current Staff. • CQC new Staff.

International transfers and legal gateway	Not Used
Plan for return and destruction of the data once the Processing is complete	The Parties are required to erase Personal Data from any computers, storage devises 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 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. Data storage and processing locations are in the United Kingdom

ANNEX 1: Exposure Critical Contract List

1. The Supplier shall:

- 1.1. provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:
 - a) are with any UK public sector bodies including central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;
 - b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or
 - c) involve or could reasonably be considered to involve CNI;
- 1.2. provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

ANNEX 2: - Corporate Resolvability Assessment (Structural Review)

1. The Supplier shall:

- 1.1 provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;
- 1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and
- 1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information and Commentary

1. The Supplier shall:

- 1.3 provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and
- 1.4 ensure that the information is presented in a simple, effective and easily understood manner.

2. For the avoidance of doubt

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

Schedule 9 - Variation Form

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

Contract Details		
This variation is between:	[insert name of Buyer] ("the Buyer") And [insert name of Supplier] ("the Supplier")	
Contract name:	[insert name of contract to be changed] ("the Contract")	
Contract reference number:	[insert contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete as applicable: Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
A Variation Impact Assessment shall be provided within:	[insert number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • [Buyer to insert original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

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

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address

Schedule 10 – Supplier Specific Terms and Conditions

1 Definitions and Interpretation

1.1. In this Schedule the following definitions apply:

Applicant:	means an individual who is the subject of a Disclosure Application
Application Form:	means the form which an Applicant must complete for the purposes of a Disclosure Application
Authorised User:	means any person authorised by the Buyer or any successor body to use the Online Account and the e-Bulk Service
Buyer Materials:	means all materials the Buyer provides to Supplier in connection with the performance of the Services (including but not limited to information, software, documentation, data and trademarks)
Buyer Representative:	means any other person appointed by the Buyer pursuant to paragraph s.1
Buyer Site:	means the Buyer's website or intranet site located at [NAME].disclosures.co.uk
Code of Practice:	means the DBS's "Code of Practice for Registered Persons and Other Recipients of Disclosure Information" published from time to time
DBS:	means the Disclosure and Barring Service (formerly the Criminal Records Bureau)
Disclosure Application:	means an application made for a DBS Disclosure Result in a format as specified by the DBS from time to time
Disclosure Result:	means the disclosure result issued by the DBS once a DBS Disclosure Application has been completed
e-Bulk Service:	means the DBS's "e-Bulk" interface and service which provides facilities that enable Disclosure Applications to be bulk-submitted electronically to the DBS and the return of information regarding the Disclosure Result by a similar means
Intellectual Property Rights:	means all intellectual property rights howsoever arising and in whatever media including (without limitation) patents, inventions, know-how, trade secrets and other confidential information, registered designs, existing and future copyright, database rights, semiconductor topography rights, trademarks, service marks, logos, domain names, business names, trade names and moral rights, anywhere in the world whether capable of being registered or not and including any registrations or applications to register any of the foregoing rights

IT Systems:	<p>means the IT systems, equipment and website operated by a party in connection with the e-Bulk Service including (without limitation) its hardware, software and communications networks</p> <p>Online Account: means the Buyer-facing element of Supplier's IT System and from which the Buyer may access to the Services using the username and password provided by Supplier</p>
Services:	<p>means the services provided by the Supplier to the Buyer to facilitate the Buyer's access to and use of an Online Account and the e-Bulk Service to process Disclosure Applications, including setting up and maintenance of an Online Account, and the support services necessary for the management of Disclosure Applications</p> <p>Supplier Representative: means any other person nominated in accordance with paragraph 5.1</p>

2 Services

- 2.1 The Supplier shall provide the Services to the Buyer on the terms set out in this Schedule subject always to the Buyer complying with its obligations under Call-Off Contract.
- 2.2 As part of the Services, the Supplier shall use reasonable endeavours to:
- 2.2.1 ensure that the Online Account is available between 9.00am – 5.00pm on any Working Day (other than in the case of scheduled maintenance);
 - 2.2.2 provide telephone help desk services, including support for Authorised Users, between 9.00am – 5.00pm on any Working Day;
 - 2.2.3 provide online guides to assist the Buyer with using the Online Account;
 - 2.2.4 respond to all material faults with the Online Account within 48 hours of the Buyer notifying the Supplier of the same; and
- 2.3 The Supplier shall:
- 2.3.1 provide the Buyer an Online Account and provide each Authorised User with a username and password to access the Online Account;
 - 2.3.2 provide access to the electronic Application Form to allow Authorised Users to enter application data into the Online Account;
 - 2.3.3 provide telephone-based support and online training to the Buyer and its Authorised Users;
 - 2.3.4 provide an identity verification section in the Online Account to enable the Authorised Users to provide details of an Applicant's identity in support of a Disclosure Application;
 - 2.3.5 provide an identity checking service which allows overseas Applicants who are not able to use the POL identity checking service to complete a face-to-face identity check with a local professional.

3 Service Availability

- 3.1 The Buyer acknowledges that the provision of the e-Bulk Service is the responsibility of the DBS and/or its third parties and, as such, the Supplier provides no warranty or assurance for the reliability or availability of the e-Bulk Service.
- 3.2 The Supplier reserves the right at its sole discretion to suspend for a period the Services and/or the Buyer's access to the e-Bulk Service in the event that:
 - 3.2.1 DBS suspends the e-Bulk Service for any reason;
 - 3.2.2 it becomes necessary to conduct any planned or emergency maintenance to Supplier's IT Systems or to undertake any investigation or works as to prevent or resolve a security issue provided that, in the case of planned maintenance, investigation or works the Buyer is given reasonable prior written notice of the same. For the avoidance of doubt no notice shall be required in respect of emergency maintenance; or
 - 3.2.3 The Supplier reasonably believes the Buyer is in Material Breach of its obligations under this Schedule and the Buyer fails to remedy that breach within 5 Working Days of receiving notice from Supplier requiring its remedy.

4 The Buyer's Obligations

- 4.1 In respect of the Services, the Buyer shall:
 - 4.1.1 comply with the Code of Practice;
 - 4.1.2 have in place all policies required by the Code of Practice as published from time to time;
 - 4.1.3 ensure that it is eligible to submit Disclosure Applications to the DBS and on reasonable request provide written confirmation of the same to the Supplier;
 - 4.1.4 only submit Disclosure Applications in respect of Applicants who are eligible for a Disclosure Result;
 - 4.1.5 ensure that all information provided in an Application Form, whether submitted through the Online Account or otherwise, is true, accurate and correct;
 - 4.1.6 be responsible for establishing and maintaining access to the Buyer Site through an internet connection using appropriate telephony and computer equipment;
 - 4.1.7 provide the Supplier with copies of the Buyer Materials and such other assistance as may be reasonably required to develop the Buyer Site to perform the Services;
 - 4.1.8 incorporate a link to the Buyer's Site at an agreed position on designated web pages on the Buyer's intranet site;
 - 4.1.9 ensure that Authorised Users use the Services and any instructions, manuals and security measures (including passwords) provided by the Supplier from time to time in accordance with this Schedule;
 - 4.1.10 be responsible for protecting the safekeeping of any passwords or log in details against unauthorised use, or disclosure to persons who are not Authorised Users;
 - 4.1.11 immediately notify the Supplier if it becomes aware of any unauthorised use or disclosure of a password. Until such notice is received by the Supplier, the Supplier shall be entitled to assume that all acts or dealings done in connection with the Services by a person who uses a password that has been provided to the Buyer is an Authorised User and accordingly constitutes an act or dealing by the Buyer; and
 - 4.1.12 to the best of its ability, ensure that the Supplier is informed of any changes in Authorised Users and provide Supplier with an up-to-date record of contact details for Authorised Users

4.2 In respect of the e-Bulk Services, the Buyer shall:

- 4.2.1 provide the Supplier with such assistance, resources and information as may be reasonably required by Supplier to:
 - i. set up, configure and test the Buyer's IT Systems to enable access to the e-Bulk Service; and
 - ii. set up, configure and test Supplier's IT Systems and processes to interface with the Buyer's IT systems.
- 4.2.2 at all times be responsible for ensuring accuracy of any data and/or Disclosure Applications submitted via the e-Bulk Service. In the event of any inaccuracies, the Buyer shall be liable to pay any additional charges imposed by the DBS or the Supplier in connection with any complaint or dispute raised by an Applicant including (without limitation) any charges for re-submission of Disclosure Applications; and
- 4.2.3 immediately report any security incidents or suspected incidents related to the e-Bulk Service and/or the Services to Supplier.

4.3 The Buyer shall not and shall not permit any person to:

- 4.3.1 use the Online Account or the Services unless they are an Authorised User;
- 4.3.2 use the Services in any configuration or for any purpose other than as set out in this Schedule;
- 4.3.3 resell, sub-licence, copy, alter, adapt, merge, modify, reverse, engineer, decompile, disassemble, create derivative works of the whole or any part of software comprised within the Services except with the Supplier's prior written consent or as permitted by law; or
- 4.3.4 use the Services in connection with the operation of a service bureau arrangement or outsourced service offering to any third party without Supplier's prior written consent; or
- 4.3.5 remove any proprietary notices, labels or marks associated with the Services.

5 Representatives

- 5.1 Both the Supplier and the Buyer shall each appoint a representative who shall be the first point of contact for each party and who shall oversee the application of this Schedule. The appointed representative shall have authority to bind its respective party in writing on all matters relating to this Schedule.

6 Confidentiality

- 6.1 The Buyer acknowledges that the information revealed in a Disclosure Result is confidential and must:
 - 6.1.1 only be shared with those of the Buyer's employees or agents who have a right to view it in the course of their specific duties in relation to recruitment and vetting processes;
 - 6.1.2 be stored, transmitted and disposed of in a secure manner;
 - 6.1.3 not be retained for any longer than necessary; and
 - 6.1.4 not be reproduced in any form, including photocopies or scanned images without the prior written Schedule of the DBS.

- 6.2 No party shall use any other party's Confidential Information for any purpose other than to perform its obligations under this Schedule.
- 6.3 The obligations of confidentiality in this paragraph 5 shall not be affected by the expiry or termination of this Schedule.

7 Licence and Intellectual Property

- 7.1 All rights, title and interest in and to the Intellectual Property Rights which are used or developed in the performance of the Services ("Supplier IPR") shall remain vested in Supplier or its licensors.
- 7.2 The Supplier hereby grants to the Buyer a personal, non-exclusive, non-transferable licence to use the Supplier IPR for the sole purpose of managing and processing Disclosure Applications for its internal business purposes in accordance with the terms of this Schedule.
- 7.3 The Buyer agrees that, following the expiry or other termination of this Contract for whatever reason, it shall not use the Supplier IPR to develop the Buyer Materials or to develop any new software or IT systems provided always that the Supplier shall be entitled acting reasonably and upon giving reasonable prior written notice to the Buyer to access the Buyer's premises to inspect any such Buyer Materials or new IT systems or software.
- 7.4 All rights, title and interest in and to the Intellectual Property Rights in the Buyer Materials shall remain vested in the Buyer or its licensors.
- 7.5 The Buyer hereby grants the Supplier a non-exclusive, royalty-free licence to use the Buyer Materials as necessary for the purpose of performing its obligations under this Schedule.
- 7.6 The Supplier shall fully indemnify the Buyer against all actions, claims, demands, proceedings, damages, costs, charges and expenses arising from or incurred by reason of any infringement or alleged infringement of any patent, registered design or copyright by the provision of the Services supplied by the Supplier, subject to the following:
- 7.6.1 the Buyer shall promptly notify the Supplier in writing of any alleged infringement of which it has notice;
 - 7.6.2 the Buyer must make no admissions without the Supplier's consent;
 - 7.6.3 the Buyer, at the Supplier's request and expense shall allow the Supplier to conduct and/or settle all negotiations and litigation and give Supplier all reasonable assistance. The costs incurred or recovered in such negotiations and litigation shall be for the Supplier's account.
- 7.7 The Buyer shall fully indemnify the Supplier both during the term and after its expiry or termination for whatever reason against all actions, claims, demands, proceedings, damages, costs, charges and expenses arising from or incurred by reason of any infringement or alleged infringement of any Intellectual Property Rights by the provision or use of the Buyer Materials supplied by the Buyer under the Schedule, subject to the following:
- 7.7.1 The Supplier shall promptly notify the Buyer in writing of any alleged infringement of which it has notice;
 - 7.7.2 The Supplier must make no admissions without the Buyer's consent;

- 7.7.3 The Supplier, at the Buyer's request and expense shall allow the Buyer to conduct and/or settle all negotiations and litigation and give the Buyer all reasonable assistance. The costs incurred or recovered in such negotiations and litigation shall be for the Buyer's account.

8 Warranties and Indemnities

8.1 The Buyer warrants that:

- 8.1.1 it, and each Authorised User, shall comply with the Code of Practice;
- 8.1.2 it shall promptly notify the Supplier of any complaint against it in respect of an alleged breach of the Code of Practice (other than complaints made spuriously or vexatiously) and any investigation into its affairs by the DBS;
- 8.1.3 all Intellectual Property Rights in and to the Buyer Materials are owned by the Buyer or its licensors and that the Supplier's use of such Intellectual Property Rights will not infringe the Intellectual Property Rights of any third parties;
- 8.1.4 it will not supply or otherwise transmit any information, data or content in connection with the Services that is or may:
 - i. contain software viruses or any other computer code, files or programmes designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment; or
 - ii. be in breach of any third-party rights (including any Intellectual Property Rights) or in violation of any applicable local or national or international law, and any regulations having the force of law.

8.2 The Buyer shall indemnify the Supplier against each loss, action, demand, cost and expense (including proper and reasonable legal fees) incurred by the Supplier as a result of or in connection with any breach by the Buyer of the terms of this Schedule.

8.3 The Supplier warrants that it will comply with all applicable national laws and regulations in connection with its obligations under this Schedule, including the Code of Practice.

8.4 The Supplier does not warrant that the Buyer's use and/or access to the Services will be uninterrupted or error free or that the Services will meet the Buyer's specific requirements.

8.5 The Supplier shall not be held responsible for any errors or omissions made intentionally or otherwise by the Applicant or the Buyer in respect of the information entered into the Application Form which is submitted to the DBS either via the Online Account using the e-Bulk Service or otherwise.

8.6 Except as set out to the contrary in this Schedule, all express or implied representations and warranties, including any implied warranty of satisfactory quality, fitness for a particular purpose or non-infringement, are hereby excluded to the fullest extent permitted by law.

9 Changes in DBS Procedures

- 9.1 The Supplier shall not be liable to the Buyer for any delay in performance or failure to perform its obligations in accordance with this Schedule where such delay or failure is due to a change in the Code of Practice, or a change in the procedures relating to the processing of Disclosure Applications by the DBS which the Supplier

could not reasonably have foreseen at the commencement date ("DBS Process Change").

9.2 Notwithstanding paragraph 9.1, if a DBS Process Change takes place the Supplier shall use reasonable endeavours to minimise any adverse impact on the performance of the Services and notify the Buyer of such impact. The Supplier reserves the right to vary the charges by a fair and equitable amount as necessary to reflect any consequential change to the Services which are required following a DBS Process Change.

10 Right of Audit

The parties agree to provide reasonable assistance and access to records or sites as may be requested by DBS and/or the other party in the event of an audit being carried out in connection with the Services.