Crown Commercial Service

G-Cloud 13 Call-Off Contract

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

G-Cloud 13 Call-Off Contract

Part A: Order Form

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

Platform service ID number	167378603532321
Call-Off Contract reference	To be confirmed
Call-Off Contract title	Provision of Support Service for Content Management System Based Applications for Cabinet Office
Call-Off Contract description	See Schedule 1 (Services)
Start date	1st July 2024
Expiry date	31st March 2025
Call-Off Contract value	The Call Off Contract Value shall not exceed £250,000.00 (ex VAT) in the period 1st March 2024 to 31st March 2025, and shall not exceed £230,000.00 (ex VAT) in the period 1st April 2025 to 31st March 2026. The absolute Call Off Contract Value shall not exceed £480,000.00 (ex VAT). **The Buyer is only committed to the Firm Price elements for the services shown in Schedule 2 (Call-Off Contract Charges)** plus any additional Services as would be agreed in Statement(s) of Work duly executed by the Parties.
Charging method	Electronic invoicing, monthly in arrears

Purchase order number	The Buyer shall confirm the Purchase order number(s) to the Supplier.

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

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

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

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

From the Buyer	The Minister for the Cabinet Office, 70 Whitehall, London, SW1A 2AS.
To the Supplier	Four Seals Digital Limited, Office 2, Tweed House, Park Lane, Swanley, Kent, BR8 8DT Company Number: 12497343
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: REDACTED TEXT under FOIA Section 40, Personal Information

Name: REDACTED TEXT under FOIA Section 40, Personal Information

Email: REDACTED TEXT under FOIA Section 40, Personal Information

For the Supplier:

Title: REDACTED TEXT under FOIA Section 40, Personal Information
Name: REDACTED TEXT under FOIA Section 40, Personal Information
Email: REDACTED TEXT under FOIA Section 40, Personal Information Phone: REDACTED TEXT under FOIA Section 40, Personal Information

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1st March 2024 and is valid for 9 (nine) months.
Ending (termination)	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). The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier two weeks written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: Lot 3: Cloud support
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: See Schedule 1 (Services)
Additional Services	See Schedule 1 (Services)
Location	The Services will be delivered remotely.
Quality Standards	See Schedule 1 (Services)
Technical Standards:	See Schedule 1 (Services)
Service level agreement:	See Schedule 1 (Services)

Onboarding	The onboarding plan for this Call-Off Contract is The Supplier shall provide the Services within the times agreed and to at least the minimum agreed standards and service levels and these will be formally accepted when completed to the satisfaction of the Buyer.

Offboarding	The offboarding plan for this Call-Off Contract is the supplier shall work with the Buyer throughout the engagement to ensure the transfer of the Services to either to Buyer or a replacement Supplier.
Collaboration agreement	Not used

Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed 125% of the Charges payable by the Buyer to the Supplier during the CallOff Contract Term. The annual total liability of the Supplier for all other Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term
Insurance	The Supplier insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law

Buyer's responsibilities	The Buyer is responsible for the set up / creation and contractual maintenance of both AWS and Github accounts.
Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes Cabinet Office-owned AWS accounts and Cabinet Office managed version control repositories (Github). Usage of Cabinet Office managed AWS accounts are required due to their security profile and protective monitoring in place. The Supplier will be provided with suitable access credentials. The Cabinet Office Github Organisation is used to ensure all codebases and IP is retained by Cabinet Office.

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 is by BACS transfer
Payment profile	The payment profile for this Call-Off Contract is monthly in arrears

Invoice details	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	Invoices will be sent to the following mailboxes: ● REDACTED TEXT under FOIA Section 43 (2), Commercial Information ● REDACTED TEXT under FOIA Section 43 (2), Commercial Information
Invoice information required	All invoices must include: ● Purchase Order Number (to be provided by Cabinet Office Digital) ● Itemisation of the work delivered, together with associated cost
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	The Call Off Contract Value shall not exceed £250,000.00 (ex VAT) in the period 1st July 2024 to 31st March 2025, and shall not exceed £230,000.00 (ex VAT) in the period 1st April 2025 to 31st March 2026. The absolute Call Off Contract Value shall not exceed £480,000.00 (ex VAT). The Buyer is only committed to the Firm Price elements for each of the services shown in Schedule 2 (Call-Off Contract Charges) plus any additional Services as would be agreed in Statement(s) of Work duly executed by the Parties.
Call-Off Contract charges	The breakdown of the Charges is shown in Schedule 2 (Call Off Charges)

Additional Buyer terms

Performance of the Service	See Schedule 1 (Services)
Guarantee	Not Used
Warranties, representations	None further those incorporated Framework Agreement clause 2.3
Supplemental requirements in addition to the Call-Off terms	Within the scope of the Call-Off Contract, the Supplier will comply with the provisions of the Security Schedule at Appendix F of Schedule 1 (Services)
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 is being used.
Intellectual Property	All code and IP assets produced by the supplier remain the IP of the Buyer.
Social Value	Not used

1. Formation of contract

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

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

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

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

2. Background to the agreement

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

Signed	Supplier	Buyer
Name		

Title		
Signature	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information
Date		

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

Full Name:REDACTED TEXT under FOIA Section 40, Personal Information Full Name: REDACTED TEXT under FOIA Section 40, Personal Information

Job Title/Role: REDACTED TEXT under FOIA Section 40, Personal Information Job Title/Role:REDACTED TEXT under FOIA Section 40, Personal Information

Date Signed: 28/06/2024 Date Signed: 28/06/2024

Customer Benefits

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

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

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

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

- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

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

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the 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 trade marks on any of its products or services without the other Party's prior written consent.

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

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

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

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the

Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

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

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

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

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

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

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

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

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles 13.6.6

Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its

unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

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

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied 18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

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

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

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

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

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

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

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

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

27.1 Except as specified in clause 29.8, a person who isn't Party to this 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

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

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

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

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

29.5.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

33.1 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

Statement of Requirements

Provision of a Support Service for Content Management System Based Applications for Cabinet Office Digital

1. PURPOSE

1.1 The Minister for the Cabinet Office seeks to secure a supplier to provide ongoing support and maintenance (on a Firm Price basis) and continuous improvement (as agreed through Statements of Work) for several Content Management System (CMS) based applications hosted on Cabinet Office Amazon Web Services (AWS). This includes both public and internal facing CMS applications.

1.2 The purpose of this document is to provide a statement of requirements for a support contract of a 9 month Initial Term from 1st July 2024 to 31st March 2025 (with an optional 12-month extension from 1st April 2025 to 31st March 2026). The scope of the support contract shall provide ongoing support, maintenance and continuous improvement for several Content Management Systems (CMS) based applications hosted on Cabinet Office AWS. These services can include both public and internal digital services.

Currently, Cabinet Office has Wagtail and WordPress based CMS applications.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Cabinet Office supports the Prime Minister and ensures the effective running of the government. The Cabinet Office is also the government's corporate headquarters, in partnership with HM Treasury, and takes the lead in certain critical policy areas. The Cabinet Office has responsibility for:

2.1.1 Supporting collective government, helping to ensure the effective development, coordination and implementation of policy

2.1.2 Supporting the National Security Council and the Joint Intelligence Organisation, coordinating the government’s response to crises and managing the UK’s cyber security

2.1.3 Promoting efficiency and reform across government through innovation, better procurement and project management, and by transforming the delivery of services

2.1.4 Promoting the release of government data, and making the way government works more transparent

2.1.5 Creating an exceptional Civil Service, improving its capability and effectiveness

2.1.6 Political and constitutional reform

2.2 The Cabinet Office Digital (CO Digital) is the department's IT and digital shared services function.

2.3 Cabinet Office Digital Delivery is the unit responsible for the build, assurance and operational support of CO Digital's portfolio of services.

3. BACKGROUND TO REQUIREMENT / OVERVIEW OF REQUIREMENT

3.1 Cabinet Office Digital Delivery is responsible for driving the delivery of digital projects for a range of business units in the Cabinet Office by using in-house crossfunctional teams, who deliver using a combination of internal resources and procured third party suppliers. Cabinet Office Digital Delivery oversees both the development and infrastructure aspects of these projects using a range of technology solutions.

3.2 A proportion of these projects support the delivery of policy and legislative objectives, including transactional websites. Others include intranets and extranets.

3.3 The audiences for these digital services are a wide user base. For intranets and extranets in scope, the users range from Civil Servants working in the Cabinet Office extending to departmental public bodies that fall under it. The public-facing websites in scope can be used by members of the public accessing information as well as individuals completing transactions on these sites with specific needs to complete certain tasks that support Cabinet Office legislation or directives.

3.4 A subset of internal administrative users within Cabinet Office business units manage the online processes for their transactional sites directly.

3.5 All these services are predominantly hosted using Amazon Web Services (AWS).

3.6 Recently, CO Digital has implemented a Wagtail-based Content Management System (CMS). Cabinet Office Digital developed a generic Wagtail based high available architecture. CO Digital built terraform-based Infrastructure as a Code (IaC) scripts to build the infrastructure. All implementations of

Wagtail-based CMS solutions will be based on this IaC. Along with the infrastructure, CO Digital has also built a Wagtail-based repository that can be forked by future implementations and used as a base. These applications might use other gov.uk services like gov.uk notify to send emails or COLA (Cabinet Office Login Application) for user authentication.

3.7 The Codebase can be shared with the Supplier upon request.

3.8 To account for complexity, risk profile, criticality and maintenance effort, CO Digital CMS services have been categorised as either 'small', 'medium' or 'large', as defined in the table below:

Category	Attributes
Small	Static, non-transactional brochure site Minimal complexity or more comprehensive integration with AWS Ecosystem services Low traffic volume
Medium	Some transactional functionality Larger user base spread across various UK Government Departments More complex in terms of AWS integrations and customised PHP code
Large	Large user base with some complexity High profile and criticality (availability requirements)

4. DEFINITIONS

Expression or Acronym	Definition
COLA	means Cabinet Office Login Application
CO Digital	means Cabinet Office Digital
CO Digital Delivery	means Cabinet Office Digital Delivery
CMS	means Content Management System
IaC	means Infrastructure as Code
AWS	means Amazon Web Services

5. SCOPE OF REQUIREMENT

5.1 The Supplier shall maintain and support the applications and infrastructure for the implementations based on the WordPress and Wagtail open source code Content Management Systems, including

5.1.1 The AWS infrastructure codes written in Terraform and the monitoring ecosystems

5.1.2 The Wagtail open source implementation

5.1.3 The frontend and backend codes

5.1.4 Custom codes for integrations to other government services, such as GOV.UK Notify and Cabinet Office Login Application (COLA)

5.1.5 Custom codes for Wagtail projects and modules

5.2 The Supplier shall fulfil all necessary tasks for

5.2.1 The support, management and remediation of issues and incidents to the Services, with appropriate Service Level Agreements as outlined in this Statement of Requirements and in accordance with agreed incident severity levels, as shown in Section 11.

5.2.2 The maintenance and patching of application and infrastructure code in accordance with the Security Schedule at Appendix A

5.2.3 The manage and reporting of security incidents in compliance with the security policies and Security Schedule as at Appendix A

5.2.4 The maintenance of the development and operation practice according to the Cabinet Office Development and Operation Strategy; the architecture needs to be approved by the Buyer's Technical Design Authority.

5.2.5 Undertake continuous improvements as and when requested by service teams or CO Digital or Portfolio Delivery. Any such activities MUST be agreed by the Parties in Statements of Work. Statements of Work MUST be executed by the Buyer's Authorised Representative ONLY. Then a Purchase Order will be raised for the executed Statement of Work. Should the Supplier undertake any unauthorised work without a Statement of Work in place for such which has been executed by the Buyer's Authorised Representative, the Supplier shall not be paid.

5.2.6 The provision of a dedicated ticket management tooling for the duration of the Contract (Service Desk software), the Supplier shall make use of

existing communications channels (Slack, Jira, email). This includes fielding queries and requests through the email distribution lists.

5.3 The Supplier shall configure appropriate availability monitoring and protective monitoring alerts using AWS CloudWatch and Pingdom. Should additional monitoring tooling be required, the Supplier shall communicate the need to Cabinet Office Digital.

5.4 Full technical details of the CMS service can be made available to the Supplier via access to the GitHub repository upon request.

5.5 The Supplier shall ensure backup procedures are scheduled for all relevant components

5.6 The Supplier shall rehearse and perform recovery routines in the event of a component failure, in line with their Business Continuity and Disaster Recovery Plan.

5.7 The Supplier shall undertake any remediations following the results of any Penetration Test. Any remediation work that doesn't need a code change shall be catered for under the Firm Prices. Where a code change is required, the Parties shall agree on the scope and the price of such in a Statement of Work.

5.8 The Supplier shall migrate the applications to AWS Lightsail by 30th September 2024. It is envisaged that all applications will need to migrate to AWS Lightsail by 30th September 2024; however, the Customer may advise the Supplier of a small number of applications which may not be suitable for Lightsail migration and shall not migrate. The Supplier shall only charge the Customer the Lightsail migration Firm Prices for those applications that have been migrated.

6. THE REQUIREMENT

The Supplier shall provide the following support and maintenance packages.

The table in this section below shows what specific package each application requires:

Service operations and maintenance - Packages

6.1 Bronze Package

Business Hours Support. Monday to Friday 09:00 to 17:00 UK time (excluding Bank Holidays in England & Wales) – which shall include:

- Maintenance and patching of core codebase runtimes and library dependencies
- Active monitoring of both the performance and availability of the service, providing additional monitoring where needed or using existing protective monitoring tools as provided by Cabinet Office
- Service Desk for error reporting, maintenance scheduling and incident response
- On-boarding of new CMS based services
- Diagnosis and remediation of P1 to P4 security incidents, issues and outages in accordance with the Service Level Agreements (SLAs)

6.2 Silver Package

Non-Business Hours Support Light – which shall include:

- Maintenance and patching of core codebase runtimes and library dependencies

- Active monitoring of both the performance and availability of the service, providing additional monitoring where needed or using existing protective monitoring tools as provided by Cabinet Office
- Service Desk for error reporting, maintenance scheduling and incident response
- On-boarding of new CMS based services
- Diagnosis and remediation of P1 security incidents, issues and outages in accordance with Service Level Agreements (SLAs). For P1 incidents, issues and outages this must be undertaken anytime on a 365/24/7 basis.
- Diagnosis and remediation of P2 to P6 security incidents, issues and outages in accordance with the Service Level Agreements (SLAs). For P2 to P6 incidents, issues and outages - support with and tickets shall be created as and when issues are raised however, they will be actioned during business hours only (i.e Monday to Friday 09:00 to 17:00 UK time, excluding Bank Holidays in England & Wales)

6.3 Gold Package

Non-Business Hours Support Full – which shall include:

- Maintenance and patching of core codebase runtimes and library dependencies
- Active monitoring of both the performance and availability of the service, providing additional monitoring where needed or using existing protective monitoring tools as provided by Cabinet Office
- Service Desk for error reporting, maintenance scheduling and incident response
- On-boarding of new CMS based services
- Diagnosis and remediation of P1-P6 security incidents, issues and outages in accordance with Service Level Agreements (SLAs). For

P1-P6 incidents, issues, and outages, this must be undertaken at any time on a 365/24/7 basis.

6.4 Service Continuous Improvement and Enhancements

Any Service Improvements and enhancements shall be undertaken by the Parties under a Statement of Work, which shall be executed by the Parties. Only the Authorised Representative of the Buyer can sign any such Statements of Work on behalf of the Cabinet Office.

6.5 The Supplier must meet the following requirements:

- The Supplier must have the accreditation and certifications as outlined in the Security Schedule, including but not limited to Cyber Essentials Plus
- The Supplier must be able to demonstrate experience delivering comparable products and services to similar organisations

6.6 Capability and Experience ● Detail the capability and resources provided for this work.

- Experience in operating and improving AWS infrastructure on AWS ECS and Fargate, CodePipeline and CodeBuild
- Experience in developing AWS infrastructure in Terraform and CloudFormation
- Experience in service operation, including developing operation runbook and incident management processes
- Experience in application development in Python and Django is desirable.

List of applications which require support

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Tier and support levels and agreed Time and Material pots can be found in Annex 1 of Schedule 2.

Should any further applications require support, this shall be agreed by the Parties as part of a Variation.

7. KEY MILESTONES AND DELIVERABLES

7.1 The following Contract milestones/deliverables shall apply:

Milestone / Deliverable	Description	Timeframe or Delivery Date
On Boarding	The Supplier will provide the Services within the agreed-upon times and to the minimum agreed-upon standards and service levels, and they will be formally accepted when completed to the satisfaction of the Buyer.	Within a week of contract award or no later than 1st July 2024
Migration	Migration of all the applications to AWS Lightsail, unless any application(s) is not to migrate to AWS Lightsail, as confirmed to the Supplier by the Buyer.	Within 3 months of contract award or no later than 30th Sept 2024
Contract Management	The Supplier will work with the Buyer and provide the Services, including agreed reports, actions, service levels, and timescales. These will be formally accepted when completed to the Buyer's satisfaction.	Throughout the Contract duration
Off Boarding Planning	The supplier will work with the Buyer throughout the engagement to ensure the transfer of relevant skills to the Cabinet Office Digital Delivery team; and Off Boarding of any application(s) in accordance with the Exit Plan.	Throughout the Contract duration

8. MANAGEMENT INFORMATION/REPORTING

8.1 Where the Supplier has agreed to deliver tasks under any Statement of Work, the Supplier shall provide updates on these tasks, including

8.1.1 Attending and presenting progress reports and updates at Monthly Service Management meetings

8.1.2 Task completion, measured against the agreed delivery date for each task

8.1.3 Current documented challenges that have potentially impacted on the delivery of agreed tasks including but not limited to:

8.1.3.1 Actions taken by the Supplier to resolve documented challenges

8.1.3.2 Estimate of delay on the agreed delivery date of the task

8.2 The Supplier shall provide data on the uptime of the service and performance against the stated SLAs.

9. QUALITY

9.1 The Supplier will deliver the Services adhering to the Gov.UK Service Standards in a way that enables the Authority to comply with its obligations under the Technology Code of Practice, which is available at https://www.gov.uk/government/publications/technology-code-of-practice/technologycode-of-practice.

9.2 Support and remediation activity should restore the service to its previous operating state and include follow-up action to prevent future occurrences.

9.3 Monitoring and performance activity should align with the broader logging process used by the platform or team.

10.PRICE

As detailed in Schedule 2.

10.4 Prices are to be submitted via email to faye.burnie@cabinetoffice.gov.uk Price Schedule excluding VAT and including all expenses relating to Contract delivery.

11. SERVICE LEVELS AND PERFORMANCE

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

Bronze Package

KPI	Service Area	KPI description	Target
1	User Support	Email or online ticketing: Response within 1 hour during Business Hours.	99%
2	Incident support	Support for P1 to P4 incidents where a part of the software or infrastructure was previously working and is not working as expected or at all.	100%
3	Issue escalation	Supplier to resolve 80% of service desk tickets without requiring the involvement of AWS Support or other affiliated partners	80%
4	Staff Security clearance	All staff to have the relevant security clearance (a minimum of BPSS)	100%
5	Availability	Services are available for users	100%

Severity level	Definition	Response time
P1 - Service Down	Core service outage	Immediate within Business Hours
P2 - Critical	Dependency outage or significant customer impact that threatens productivity	Within 1 hour within Business Hours
P3 - Urgent	High-impact issue that significantly impairs service operation; there is a timesensitive issue affecting long term productivity but not causing an immediate service outage	Within 2 hours within Business Hours

P4 - Important	Important issues that do not have significant productivity or operational impact. Requires necessary remediation	Within 4 hours within Business Hours

Silver Package

KPI	Service Area	KPI description	Target
1	User Support	Email or online ticketing: Response within 1 hour during Business Hours (or in the case of a ticket relating to P1 issue on a 365/24/7 basis).	99%
2	Incident support	Support for P1 to P6 incidents where a part of the software or infrastructure was previously working and is not working as expected or at all.	100%
3	Issue escalation	Supplier to resolve 80% of service desk tickets without requiring the involvement of AWS Support or other affiliated partners	80%
4	Staff Security clearance	All staff to have the relevant security clearance (a minimum of BPSS)	100%
5	Availability	Services are available for users	100%

Severity level	Definition	Response time
P1 - Service Down	Core service outage	Immediate on a 365/24/7 basis
P2 - Critical	Dependency outage or significant customer impact that threatens productivity	Within 1 hour within Business Hours

P3 - Urgent	High-impact issue that significantly impairs service operation; there is a timesensitive issue affecting long term productivity but not causing an immediate service outage	Within 2 hours within Business Hours
P4 - Important	Important issue that does not have significant productivity or operational impact. Requires necessary remediation	Within 4 hours within Business Hours
P5 - Monitor	Issue requiring no further action beyond monitoring for follow-up, if needed	Within 1 business day
P6 - Informational	Request for information only	Within 1 business day

Gold Package

KPI	Service Area	KPI description	Target
1	User Support	Email or online ticketing: Response within 1 hour at any time.	99%
2	Incident support	Support for P1 to P6 incidents where a part of the software or infrastructure was previously working and is not working as expected or at all.	100%
3	Issue escalation	Supplier to resolve 80% of service desk tickets without requiring the involvement of AWS Support or other affiliated partners	80%

4	Staff Security clearance	All staff to have the relevant security clearance (a minimum of BPSS)	100%
5	Availability	Services are available for users	100%

Severity level	Definition	Response time
P1 - Service Down	Core service outage	Immediate at any time
P2 - Critical	Dependency outage or significant customer impact that threatens productivity	Within 1 hour at any time
P3 - Urgent	High-impact issue that significantly impairs service operation; there is a timesensitive issue affecting long term productivity but not causing an immediate service outage	Within 2 hours at any time
P4 - Important	Important issue that does not have significant productivity or operational impact. Requires necessary remediation	Within 4 hours at any time
P5 - Monitor	Issue requiring no further action beyond monitoring for follow-up, if needed	Within 1 business day
P6 - Informational	Request for information only	Within 1 business day

Business Hours are defined as Monday to Friday, 09:00 to 17:00 (UK time), excluding Bank Holidays in England & Wales

12. SECURITY AND CONFIDENTIALITY REQUIREMENTS

12.1 The Supplier shall ensure that all staff delivering the Services hold UK National Security Vetting to "BPSS" level, as a minimum.

12.2 The Supplier shall support annual penetration tests of their code at least annually by a third-party CHECK-accredited organisation. Penetration testing will be arranged and coordinated by CO Digital

12.3 The Supplier shall work with Cabinet Office Digital Delivery to ensure that their coding follows security best practices.

12.4 The Supplier shall ensure that any third parties used by it in the course of the service provision and deemed critical to the Services shall adopt a systematic approach to managing information so that it remains secure.

12.5 The Supplier shall ensure that they adhere to the Security Schedule detailed in Appendix A. In the case of any conflict between this Statement of Requirements and the Security Schedule, the Security Schedule, as in Appendix A, shall take precedence.

13. PAYMENT AND INVOICING

13.1 The payment profile for this Call-Off Contract is monthly in arrears.

13.2 A Purchase Order will be raised once the Contract has been signed for the Firm Price elements. Separate POs will be raised for each Statement of Work.

13.3 The Buyer commits to the Firm Price scope and will commit to any Statement(s) of Work entered into. The Buyer reserves the right to request additional applications are 'onboarded' and/or applications are 'off-boarded', by providing the Supplier with at least two weeks notice. Any such additional 'onboarding' or 'offboarding' shall be agreed between the Parties in a Contract Change Notice.

13.4 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables. Where T&M work takes place without a valid Statement of Work being duly executed by the Buyer's Authorised Representative, the Buyer will not accept any invoice for such.

13.5 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs. Such costs must be in accordance with Contract

13.6 The Supplier shall submit invoices in PDF format by email to REDACTED TEXT under FOIA Section 43 (2), Commercial Information

13.7 All Invoices must include a valid PO number. Any duly executed Statement of Work will have its own PO. Each invoice must be accompanied by a breakdown of the deliverables and services, quantity thereof, applicable unit charges, split by application and the total charge for the invoice period in sufficient detail to enable the Customer to validate the invoice.

14. CONTRACT MANAGEMENT

14.1 The Supplier will facilitate monthly (or as otherwise agreed) status review meetings between Cabinet Office Digital Delivery and the Supplier.

14.2 These meetings shall be held virtually, but where a physical meeting is requested by the Cabinet Office, attendance at status review meetings shall be at the Supplier's own expense.

15. LOCATION

15.1 The Services will be delivered to the Cabinet Office

1 Horse Guards Road London

ANNEX F

Schedule (Security Management): (Developer)

Buyer Options

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

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

1 Buyer risk assessment

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

(a) comply with all requirements of this Schedule (*Security Management*); and

(b) hold the ISO/IEC 27001:2013 Relevant Certification from a UKAS-approved certification body (see Paragraph 8).

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

(a) Paragraph 9 (*Security Management Plan*);
(b) paragraph 9 of the Security Requirements (*Code Reviews*);

(c) paragraph 11 of the Security Requirements (*Third-party Software Modules*);

(d) paragraph 12 of the Security Requirements (*Hardware and software support*);

(e) paragraph 13 of the Security Requirements (*Encryption*); and

(f) paragraph 19 of the Security Requirements (*Access Control*).

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

2 Definitions

2.1 In this Schedule (*Security Management*):

"Anti-virus Software"	means software that: (a) protects the Supplier Information Management System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier Information Management System; (c) if Malicious Software is detected in the Supplier Information Management System, so far as possible: (i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier Information Management System;
"Breach Action Plan"	means a plan prepared under paragraph 22.3 of the Security Requirements addressing any Breach of Security;
"Breach of Security"	means the occurrence of:
	(a) any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code; (d) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code; and/or (e) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;

	(f) the installation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; (g) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the: (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System; and (h) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: (i) was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom
"Buyer Data"	means any: (a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; (b) Personal Data for which the Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in paragraphs (a) or (b); that is: (a) supplied to the Supplier by or on behalf of the Buyer; or (b) that the Supplier generates, processes, stores or transmits under this Agreement; and for the avoidance of doubt includes the Code and any meta-data relating to the Code.

"Buyer Data Register"	means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 23 of the Security Requirements;
"Buyer Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
"Buyer System"	means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services;

"Certification Default"	means the occurrence of one or more of the circumstances listed in Paragraph 8.4;
"Certification Rectification Plan"	means the plan referred to in Paragraph 8.5(a);
"Certification Requirements"	means the requirements set out in paragraph 8.3.
"CHECK Scheme"	means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks
"CHECK Service Provider"	means a company which, under the CHECK Scheme: (a) has been certified by the National Cyber Security Centre; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by paragraph 18 of the Security Requirements;
"Code"	means, in respect of the Developed System: (a) the source code; (b) the object code; (c) third-party components, including third-party coding frameworks and libraries; and (d) all supporting documentation.
"Code Review"	means a periodic review of the Code by manual or automated means to: (a) identify and fix any bugs; and (b) ensure the Code complies with: (i) the requirements of this Schedule (*Security Management*); and (ii) the Secure Development Guidance;
"Code Review Plan"	means the document agreed with the Buyer under paragraph 9.3 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews;
"Code Review Report"	means a report setting out the findings of a Code Review;
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;

"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;

“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
“Developed System”	means the software or system that the Supplier will develop under this Agreement;
“Development Activity”	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (c) code storage; and (d) deployment.
“Development Environment”	means any information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Development Activity;
“EEA”	means the European Economic Area;
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
“Email Service”	means a service that will send, or can be used to send, emails from the Buyer’s email address or otherwise on behalf of the Buyer;
“HMG Baseline Personnel Security Standard”	means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time;
“IT Health Check”	means security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment in accordance with paragraph 33 of the Security Requirements;
“Malicious Software”	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
“Modules Register”	means the register of Third-party Software Modules required for higher risk agreements by paragraph 11.3 of the Security Requirements;
“NCSC”	means the National Cyber Security Centre;

"NCSC Cloud Security Principles"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles.
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;

"NCSC Protecting Bulk Personal Data Guidance"	means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
"NCSC Secure Design Principles"	means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles.
"OWASP"	means the Open Web Application Security Project Foundation;
"OWASP Secure Coding Practice"	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-referenceguide/migrated_content;
"OWASP Top Ten"	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/;
"Privileged User"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"Process"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
"Prohibited Activity"	means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice;
"Prohibition Notice"	means a notice issued under paragraph 1.8 of the Security Requirements.
"Protective Monitoring System"	means the system implemented by the Supplier and its Sub-contractors under paragraph 20.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code

"Register of Support Locations and ThirdParty Tools"	means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools: (a) the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable); (b) where that activity is performed by individuals, the place or facility from where that activity is performed; and (c) in respect of the entity providing the Support Locations or Third-Party Tools, its: (i) full legal name; (ii) trading name (if any) (iii) country of registration; (iv) registration number (if applicable); and (v) registered address.
"Relevant Activities"	means those activities specified in paragraph 0 of the Security Requirements.

"Relevant Certifications"	means (a) in the case of a standard agreement: (i) Cyber Essentials; and/or (ii) Cyber Essentials Plus as determined by the Buyer; or (b) in the case of a higher risk agreement: (i) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and (ii) Cyber Essentials Plus;
"Relevant Convictions"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify
"Remediation Action Plan"	means the plan prepared by the Supplier in accordance with Paragraph 18.11 to 18.15, addressing the vulnerabilities and findings in a IT Health Check report

"Secure Development Guidance"	means: (a) the NCSC's document "Secure development and deployment guidance" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/developers-collection; and (b) the OWASP Secure Coding Practice as updated or replaced from time to time;
"Security Management Plan"	means the document prepared in accordance with the requirements of Paragraph 9 and in the format, and containing the information, specified in Annex 2.
"SMP Sub-contractor"	means a Sub-contractor with significant market power, such that: (a) they will not contract other than on their own contractual terms; and (b) either: (i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or (ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services.
"Sites"	means any premises: (a) from or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or
	(b) where: (i) any part of the Supplier Information Management System is situated; or (ii) any physical interface with the Buyer System takes place; and (c) for the avoidance of doubt include any premises at which Development Activities take place
"Sub-contractor"	includes, for the purposes of this Schedule (*Security Management*), any individual or entity that: (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data;
"Sub-contractor Personnel"	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and

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

3 Introduction

3.1 This Schedule (*Security Management*) sets out:

(a) the assessment of this Agreement as either a:

(i) higher risk agreement; or

(ii) standard agreement,

in Paragraph 1;

(b) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of:

(i) the Development Activity;

(ii) the Development Environment;

(iii) the Buyer Data;

(iv) the Services; and

(v) the Supplier Information Management System;

(c) the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;

(d) the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 7;

(e) the Certification Requirements, in Paragraph 8;

(f) the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 9; and

(g) the Security Requirements with which the Supplier and its Sub-contractors must comply.

4 Principles of Security

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

(a) the Sites;

(b) the Services; and

(c) the Supplier's Information Management System.

4.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 5.1.

4.3 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:

(a) the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors;

(b) the security and integrity of the Developed System; and

(c) the security of the Supplier Information Management System.

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

5 Security Requirements

5.1 The Supplier shall:

(a) comply with the Security Requirements; and

(b) subject to Paragraph 6.2, ensure that all Sub-contractors also comply with the Security Requirements.

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

(a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;

(b) document the differences between Security Requirements the obligations that the SMP Subcontractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;

(c) take such steps as the Buyer may require to mitigate those risks.

6 Access to Supplier Personnel and Supplier Information Management System

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

(a) access to the Supplier Personnel, including, for the avoidance of doubt, the Sub-contractor Personnel;

(b) access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Sub-contractor; and

(c) such other information and/or documentation that the Buyer or its authorised representatives may require,

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

6.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 7.1: (a)

in the case of a Breach of Security within 24 hours of such a request; and

(b) in all other cases, within 10 Working Days of such request.

7 Certification Requirements

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

(a) it; and

(b) any Sub-contractor,

is certified as compliant with the Relevant Certifications.

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

(a) the Relevant Certifications for it and any Sub-contractor; and

(b) in the case of a higher-risk agreement, any relevant scope and statement of applicability required under the ISO/IEC 27001:2013 Relevant Certifications.

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

(a) currently in effect;

(b) cover at least the full scope of the Supplier Information Management System; and

(c) are not subject to any condition that may impact the provision of the Services or the Development Activity (the "Certification Requirements").

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

(a) a Relevant Certification has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification expired and has not been renewed by the Supplier;

(c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or

(d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "Certification Default")

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

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 8.4 (or such other period as the Parties may agree) provide a draft plan (a "Certification Rectification Plan") to the Buyer setting out:

(i) full details of the Certification Default, including a root cause analysis;

(ii) the actual and anticipated effects of the Certification Default;

(iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;

(b) the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

(c) if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph (b) will apply to the re-submitted plan;

(d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

(e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

8 Security Management Plan

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

Preparation of Security Management Plan

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

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

(a) an assessment of the Supplier Information Management System against the requirements of this Schedule (*Security Management*), including the Security Requirements;

(b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System. the Buyer Data, the Buyer, the Services and/or users of the Services; and

(c) the following information, so far as is applicable, in respect of each Sub-contractor:

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any);

(C) registration details (where the Sub-contractor is not an individual);

(ii) the Relevant Certifications held by the Sub-contractor;

(iii) the Sites used by the Sub-contractor;

(iv) the Development Activity undertaken by the Sub-contractor;

(v) the access the Sub-contractor has to the Development Environment;

(vi) the Buyer Data Processed by the Sub-contractor;

(vii) the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

(viii) the measures the Sub-contractor has in place to comply with the requirements of this Schedule (*Security Management*);

(d) the Register of Support Locations and Third Party Tools;

(e) the Modules Register;

(f) the Support Register;

(g) details of the steps taken to comply with:

(i) the Secure Development Guidance; and

(ii) the secure development policy required by the ISO/IEC 27001:2013 Relevant Certifications;

(h) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 20 of the Security Requirements, including:

(i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System and the Development environment; and

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

Approval of Security Management Plan

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

(a) an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to:

(i) undertake the Development Activity; and/or

(ii) Process Buyer Data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

8.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

8.6 The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

Updating Security Management Plan

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

Monitoring

8.8 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Supplier Information Management System;

(b) a new risk to the components or architecture of the Supplier Information Management System;

(c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

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

(h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

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

Annex 1 Security Requirements

1 Location

Location for Relevant Activities

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

(a) undertake the Development Activity;

(b) host the Development Environment; and

(c) store, access or process Buyer Data,

(the "Relevant Activities") only in the geographic areas permitted by the Buyer.

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

(a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8.

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

(i) the security controls in places at the relevant location or locations; and

(ii) where certain security controls are not, or only partially, implemented the reasons for this;

(b) the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

(c) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:

(i) cease to store, access or process Buyer Data at that location or those locations;

(ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or process Buyer Data at that location, or those locations, as the Buyer may specify.

Support Locations

1.4 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.

1.5 Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Authority has not given the Supplier notice under paragraph 1.8.

Third-party Tools

1.6 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.

1.7 The Supplier must not, and must not allow Sub-contractors to, use a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

Prohibited Activities

1.8 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a "Prohibited Activity").

(a) in any particular country or group of countries;

(b) in or using facilities operated by any particular entity or group of entities; or

(c) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,

(a "Prohibition Notice").

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

2 Vetting, Training and Staff Access

Vetting before performing or managing Services

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

(a) Development Activity;

(b) any activity that provides access to the Development Environment; or

(c) any activity relating to the performance and management of the Services

unless:

(d) that individual has passed the security checks listed in paragraph 2.2; or

(e) the Buyer has given prior written permission for a named individual to perform a specific role.

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

(a) the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

(i) the individual's identity;

(ii) the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

(iii) the individual's previous employment history; and

(iv) that the individual has no Relevant Convictions;

(b) national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

(c) such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

Annual training

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

(a) General training concerning security and data handling; and

(b) Phishing, including the dangers from ransomware and other malware.

Staff access

2.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

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

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected

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

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

3 End-user Devices

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

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

(b) users must authenticate before gaining access;

(c) all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;

(d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data and Code to ensure the security of that Buyer Data and Code;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data or Code stored on the device and prevent any user or group of users from accessing the device;

(g) all End-user Devices are within the scope of any Relevant Certification.

3.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

3.3 Where there is any conflict between the requirements of this Schedule (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

4 Secure Architecture

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

(a) the NCSC's guidance on "Security Design Principles for Digital Services";

(b) where the Developed System will Process bulk data, the NCSC's guidance on "Bulk Data Principles"; and

(c) the NCSC's guidance on "Cloud Security Principles".

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

5 Secure Software Development by Design

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

(a) no malicious code is introduced into the Developed System or the Supplier Information Management System.

(b) the Developed System can continue to function in accordance with the Specification:

(i) in unforeseen circumstances; and

(ii) notwithstanding any attack on the Developed System using common cyber-attack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

5.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity: (a)

comply with the Secure Development Guidance as if its requirements were terms of this Contract; and

(b) document the steps taken to comply with that guidance as part of the Security Management Plan.

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

(a) ensure that all Supplier Staff engaged in Development Activity are:

(i) trained and experienced in secure by design code development;

(ii) provided with regular training in secure software development and deployment;

(b) ensure that all Code:

(i) is subject to a clear, well-organised, logical and documented architecture;

(ii) follows OWASP Secure Coding Practice

(iii) follows recognised secure coding standard, where one is available;

(iv) employs consistent naming conventions;

(v) is coded in a consistent manner and style;

(vi) is clearly and adequately documented to set out the function of each section of code;

(vii) is subject to appropriate levels of review through automated and non-automated methods both as part of:

(A) any original coding; and

(B) at any time the Code is changed;

(c) ensure that all Development Environments:

(i) protect access credentials and secret keys;

(ii) are logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;

(iii) require multi-factor authentication to access;

(iv) have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;

(v) use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System;

6 Code Repository and Deployment Pipeline

7 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:

7.1 when using a cloud-based code depository for the deployment pipeline, use only a cloud-based code depository that has been assessed against the NCSC Cloud Security Principles;

7.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;

7.3 ensure secret credentials are separated from source code.

7.4 run automatic security testing as part of any deployment of the Developed System.

8 Development and Testing Data

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

9 Code Reviews

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

9.2 The Supplier must:

(a) regularly; or

(b) as required by the Buyer review the Code in accordance with the requirements of this paragraph 9 (a "Code Review").

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

(a) the modules or elements of the Code subject to the Code Review;

(b) the development state at which the Code Review will take place; (c) any specific security vulnerabilities the Code Review will assess; and

(d) the frequency of any Code Reviews (the "Code Review Plan").

9.4 For the avoidance of doubt, the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.

9.5 The Supplier:

(a) must undertake Code Reviews in accordance with the Code Review Plan; and

(b) may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.

9.6 No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the Code Review Report.

9.7 Where the Code Review identifies any security vulnerabilities, the Supplier must:

(a) remedy these at its own cost and expense;

(b) ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and

(c) modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and

(d) provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 9.7.

10 Third-party Software

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

11 Third-party Software Modules

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

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

(a) verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;

(b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;

(c) continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;

(d) take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.

11.3 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the "Modules Register").

11.4 The Modules Register must include, in respect of each Third-party Software Module:

(a) full details of the developer of the module;

(b) the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;

(c) any recognised security vulnerabilities in the Third-party Software Module; and

(d) how the Supplier will minimise the effect of any such security vulnerability on the Developed System.

11.5 The Supplier must:

(a) review and update the Modules Register:

(i) within 10 Working Days of becoming aware of a security vulnerability in any Third-party Software Module; and

(ii) at least once every 6 (six) months;

(b) provide the Buyer with a copy of the Modules Register: (i) whenever it updates the Modules Register; and (ii) otherwise when the Buyer requests.

12 Hardware and software support

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

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

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

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

(a) the date, so far as it is known, that the item will cease to be in mainstream security support; and (b)

the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.

12.5 The Supplier must:

(a) review and update the Support Register:

(i) within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;

(ii) within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and

(iii) at least once every 12 (twelve) months;

(b) provide the Buyer with a copy of the Support Register: (i) whenever it updates the Support Register; and

(ii) otherwise when the Buyer requests.

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

(a) those elements are always in mainstream or extended security support from the relevant vendor; and

(b) the COTS Software is not more than one version or major release behind the latest version of the software.

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

(a) regular firmware updates to the hardware; and

(b) a physical repair or replacement service for the hardware.

13 Encryption

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

13.2 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 13.

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

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

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

(b) when the buyer Data is transmitted.

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

(a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

(b) when transmitted.

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

(a) immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;

(c) provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.

13.7 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.

13.8 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

(a) the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;

(b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.

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

14 Email

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

supports transport layer security ("TLS") version 1.2, or higher, for sending and receiving emails;

(b) supports TLS Reporting ("TLS-RPT");

(c) is capable of implementing:

(i) domain-based message authentication, reporting and conformance ("DMARC");

(ii) sender policy framework ("SPF"); and

(iii) domain keys identified mail ("DKIM"); and

(d) is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:

(i) the UK Government (current version at https://www.gov.uk/guidance/set-up-government-emailservices-securely; or

(ii) the NCSC (current version at https://www.ncsc.gov.uk/collection/email-security-and-antispoofing).

15 DNS

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

16 Malicious Software

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

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

(a) prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;

(b) is configured to perform automatic software and definition updates;

(c) provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update's release by the vendor;

(d) performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and

(e) where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

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

16.4 The Supplier must at all times, during and after the Term, on written demand indemnify the Buyer and keep the Buyer indemnified, against all Losses incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Sub-contractor, to comply with this paragraph .

17 Vulnerabilities

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

(a) seven (7) days after the public release of patches for vulnerabilities classified as "critical";

(b) thirty (30) days after the public release of patches for vulnerabilities classified as "important"; and

(c) sixty (60) days after the public release of patches for vulnerabilities classified as "other".

17.2 The Supplier must:

(a) scan the Supplier Information Management System and the Development Environment at least once every month to identify any unpatched vulnerabilities; and

(b) if the scan identifies any unpatched vulnerabilities ensure they are patched in accordance with paragraph 17.1.

17.3 For the purposes of this paragraph 17, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as "critical", "important" or "other" that is aligned to recognised vulnerability assessment systems, such as:

(a) the National Vulnerability Database's vulnerability security ratings; or

(b) Microsoft's security bulletin severity rating system.

18 Security testing

Responsibility for security testing

18.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 18 (unless the Buyer gives notice under Paragraph 18.2); and

(b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

Security tests by Buyer

18.2 The Buyer may give notice to the Supplier that the Buyer will undertake the security testing required by Paragraph 18.4(a) and 18.4(d).

18.3 Where the Buyer gives notice under Paragraph 18.2:

(a) the Supplier shall provide such reasonable co-operation as the Buyer requests, including:

(i) such access to the Supplier Information Management System as the Buyer may request; and

(ii) such technical and other information relating to the Information Management System as the Buyer requests;

(b) the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and

(c) for the purposes of Paragraphs 18.8 to 18.17:

(i) the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and

(ii) the time limits in Paragraphs 18.8 and 18.11 run from the date on which the Buyer provides the Supplier with the copy of the report under Paragraph (b).

Security tests by Supplier

18.4 The Supplier must:

(a) during the testing of the Developed System and before the Developed System goes live (unless the Buyer gives notice under Paragraph 18.2);

(b) at least once during each Contract Year; and (c) when required to do so by the Buyer; undertake the

following activities:

(d) conduct security testing of the Developed System and the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an "IT Health Check") in accordance with Paragraph 18.5 to 18.7; and

(e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 18.8 to 18.17.

IT Health Checks

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

(a) use only a CHECK Service Provider to perform the IT Health Check;

(b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier Information Management System and the delivery of the Services.

(c) promptly provide the Buyer with such technical and other information relating to the Information Management System as the Buyer requests;

(d) include within the scope of the IT Health Check such tests as the Buyer requires;

(e) agree with the Buyer the scope, aim and timing of the IT Health Check.

18.6 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.

18.7 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

Remedying vulnerabilities

18.8 In addition to complying with Paragraphs 18.4 to 18.17, the Supplier must remedy:

(a) any vulnerabilities classified as critical in the IT Health Check report within 5 Working Days of becoming aware of the vulnerability and its classification;

(b) any vulnerabilities classified as high in the IT Health Check report within 1 month of becoming aware of the vulnerability and its classification; and

(c) any vulnerabilities classified as medium in the IT Health Check report within 3 months of becoming aware of the vulnerability and its classification.

18.9 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in the IT Health Check report within the time periods specified in Paragraph 18.8.

Significant vulnerabilities

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

Responding to an IT Health Check report

18.11 Where the IT Health Check identifies vulnerabilities in, or makes findings in respect of, the Information Management System, the Supplier must within 20 Working Days of receiving the IT Health Check report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the "Remediation Action Plan").

18.12 Where the Buyer has commissioned a root cause analysis under Paragraph 18.10, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

18.13 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the IT Health Check report:

(a) how the vulnerability or finding will be remedied;

(b) the date by which the vulnerability or finding will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.

18.14 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

18.15 The Buyer may:

(a) reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 18.13 to 18.15 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;

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

Implementing an approved Remediation Action Plan

18.16 In implementing the Remediation Action plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

18.17 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

(a) provide the Buyer with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

19 Access Control

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

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

(a) identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;

(b) require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

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

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-user Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

(e) automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) in the case of a higher-risk agreement are:

(i) restricted to a single role or small number of roles;

(ii) time limited; and

(iii) restrict the Privileged User's access to the internet.

19.4 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.

19.5 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.

19.6 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 19.2 to 19.5.

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

(a) configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and

(b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

20 Event logging and protective monitoring

Protective Monitoring System

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

(a) identify and prevent potential Breaches of Security;

(b) respond effectively and in a timely manner to Breaches of Security that do occur;

(c) identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the "Protective Monitoring System").

20.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier Information Management system; and

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Buyer Data;

(c) the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;

(d) any other matters required by the Security Management Plan.

Event logs

20.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log: (a) personal data,

other than identifiers relating to users; or

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

Provision of information to Buyer

20.4 The Supplier must provide the Buyer on request with:

(a) full details of the Protective Monitoring System it has implemented; and

(b) copies of monitoring logs and reports prepared as part of the Protective Monitoring System.

Changes to Protective Monitoring System

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

(a) respond to a specific threat identified by the Buyer;

(b) implement additional audit and monitoring requirements; and

(c) stream any specified event logs to the Buyer's security information and event management system.

21 Audit rights

Right of audit

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

(a) verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Schedule (*Security Management*) and the Data Protection Laws as they apply to Buyer Data;

(b) inspect the Supplier Information Management System (or any part of it); (c) review the integrity, confidentiality and security of the Buyer Data; and/or

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

21.2 Any audit undertaken under this Paragraph 21:

(a) may only take place during the Term and for a period of 18 months afterwards; and

(b) is in addition to any other rights of audit the Buyer has under this Agreement.

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

(a) the Supplier or any Sub-contractor has not complied with its obligations under this Agreement or the Data Protection Laws as they apply to the Buyer Data;

(b) there has been or is likely to be a Security Breach affecting the Buyer Data or the Code; or

(c) where vulnerabilities, or potential vulnerabilities, in the Code have been identified by: (i) an IT Health Check; or

(ii) a Breach of Security.

Conduct of audits

21.4 The Authority must use reasonable endeavours to provide 15 Working Days' notice of an audit.

21.5 The Authority must when conducting an audit:

(a) comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Suppler Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and

(b) use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

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

(a) all information requested by the Buyer within the scope of the audit;

(b) access to the Supplier Information Management System; and

(c) access to the Supplier Staff.

Response to audit findings

21.7 Where an audit finds that:

(a) the Supplier or a Sub-contractor has not complied with this Agreement or the Data Protection Laws as they apply to the Buyer Data; or

(b) there has been or is likely to be a Security Breach affecting the Buyer Data

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

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

22 Breach of Security

Reporting Breach of Security

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

Immediate steps

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

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

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

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

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

Subsequent action

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

(a) full details of the Breach of Security; and

(b) if required by the Buyer:

(i) a root cause analysis; and

(ii) a draft plan addressing the root cause of the Breach of Security

(the "Breach Action Plan").

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

(a) how the issue will be remedied;

(b) the date by which the issue will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.

22.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.

22.6 The Buyer may:

(a) reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 22.5 and 22.6 shall apply to the revised draft Breach Action Plan;

(b) accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

Assistance to Buyer

22.7 Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction.

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

Reporting of Breach of Security to regulator

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

(a) make that report within the time limits:

(i) specified by the relevant regulator; or

(ii) otherwise required by Law;

(b) to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.

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

(a) provide such information and other input as the Buyer requires within the timescales specified by the Buyer;

(b) where Paragraph 7 applies to the Breach of Security, ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

23 Return and Deletion of Buyer Data

23.1 The Supplier must create and maintain a register of:

(a) all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and

(b) those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-contractor, on which the Buyer Data is stored (the "Buyer Data Register").

23.2 The Supplier must:

(a) review and update the Buyer Data Register:

(i) within 10 Working Days of the Supplier or any Sub-contractor changes to those parts of the Supplier Information Management System on which the Buyer Data is stored;

(ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;

(iii) at least once every 12 (twelve) months; and

(b) provide the Buyer with a copy of the Buyer Data Register: (i) whenever it updates the Buyer Data Register; and

(ii) otherwise when the Buyer requests.

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

(a) when requested to do so by the Buyer; and

(b) using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

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

(a) when requested to do so by the Buyer; and (b) using the method specified by the Buyer.

Schedule 2: Call-Off Contract charges

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

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Annex 1 of Schedule 2 contains the services and the level of size, and support level for each service. In addition a small pot of T&M has been preapproved for use as instructed by the buyer for small incremental development work and security patching. Under no circumstances must the cap detailed in Annex 1 Schedule 2 be exceeded without a change notice issued and signed by authorised representatives for both parties.

Additional Services may be commissioned via Statement of Work (SoW). A pot of funding will be included by the Buyer in the overall Contract Value, which can be drawn down upon through the execution of SoWs. A SoW may either be Firm Price or Time & Materials. Any T&M work will be based on a blended Day Rate. Under no circumstance shall the Supplier commence work on additional services without a SoW being signed

These fixed prices include all costs for additional monitoring, professional services, and any other costs.

The day rate is a blended day rate for improvement work that falls outside of the scope of the core support requirement described in sections 5 and 6 of the requirements in schedule 1.

The pricing for onboarding and migration to LightSail and for business hours support, 24X7 Light support and 24X7 Full support as detailed in the sections 5 and 6 Prices should be categorised as small/medium/large (see section 3.9 for definition of category) of the requirement detailed in schedule 1.

Schedule 3: Collaboration agreement- NOT USED

This agreement is made on [enter date] between:

1) [Buyer name] of [Buyer address] (the Buyer)

2) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

3) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

4) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

5) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

6) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address] together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

- Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
- Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

1.1.1 “Agreement” means this collaboration agreement, containing the Clauses and Schedules

1.1.2 “Call-Off Contract” means each contract that is let by the Buyer to one of the Collaboration Suppliers

1.1.3 “Contractor’s Confidential Information” has the meaning set out in the Call-Off Contracts

1.1.4 “Confidential Information” means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information

1.1.5 “Collaboration Activities” means the activities set out in this Agreement

1.1.6 “Buyer Confidential Information” has the meaning set out in the Call-Off Contract

1.1.7 “Default” means any breach of the obligations of any Collaboration Supplier or any Default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties 1.1.8 “Detailed Collaboration Plan” has the meaning given in clause 3.2

1.1.9 “Dispute Resolution Process” means the process described in clause 9

1.1.10 “Effective Date” means [insert date]

1.1.11 “Force Majeure Event” has the meaning given in clause 11.1.1

1.1.12 “Mediator” has the meaning given to it in clause 9.3.1

1.1.13 “Outline Collaboration Plan” has the meaning given to it in clause 3.1

1.1.14 “Term” has the meaning given to it in clause 2.1

1.1.15 "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent reenactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the "Term").

2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the "Outline Collaboration Plan").

3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the "Detailed Collaboration Plan"). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier's respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.

3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.

3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:

3.4.1 approve the Detailed Collaboration Plan
3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection

3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.

3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.

4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.

4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all cooperation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.

5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

6.2 Each Collaboration Supplier warrants that:

6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party

6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors

6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise

6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:

6.3.1 or becomes public knowledge other than by breach of this clause 6

6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party

6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure

6.3.4 independently developed without access to the Confidential Information

6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction

6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

7.1 Each Collaboration Supplier warrant and represent that:

7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of

statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£,000)].

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage
8.5.2 special loss or damage
8.5.3 consequential loss or damage
8.5.4 loss of profits (whether direct or indirect)
8.5.5 loss of turnover (whether direct or indirect)
8.5.6 loss of business opportunities (whether direct or indirect)
8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.

9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.

9.3 The process for mediation and consequential provisions for mediation are:

9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties

that he is unable or unwilling to act, apply to the President of the Law Society to appoint a Mediator

9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations

9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings

9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives

9.3.5 failing agreement, any of the parties may invite the Mediator to provide a nonbinding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression “Force Majeure Event” will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the Subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals):
Position: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals): Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals): Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals): Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals): Position:
Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):
Position: Date:

Collaboration Agreement Schedule 1: List of contracts

Collaboration supplier	Name/reference of contract	Effective date of contract

Collaboration Agreement Schedule 2 [Insert Outline Collaboration Plan]

Schedule 4: Alternative clauses- NOT USED

1. Introduction

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

2. Clauses selected

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

2.1.1 Scots Law and Jurisdiction

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

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

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

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

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

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

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

2.3 Discrimination

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

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006

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

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

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

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

2.4 Equality policies and practices

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

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

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

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

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

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or

B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

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

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

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

2.5 Equality

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

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

2.6 Health and safety

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

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

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

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

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

2.7 Criminal damage

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

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

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

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

Schedule 5: Guarantee- NOT USED

[A Guarantee should only be requested if the Supplier's financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary's requirements]

This deed of guarantee is made on [insert date, month, year] between:

(1) [Insert the name of the Guarantor] a company incorporated in England and Wales with number [insert company number] whose registered office is at [insert details of the guarantor's registered office] [or a company incorporated under the Laws of [insert country], registered in [insert country] with number [insert number] at [insert place of registration], whose principal office is at [insert office details]]('Guarantor'); in favour of and

(2) The Buyer whose offices are [insert Buyer's official address] ('Beneficiary') Whereas:

(A) The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.

(B) It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn't needed then the section below and other references to the guarantee should be deleted.

Suggested headings are as follows:

- Demands and notices
- Representations and Warranties
- Obligation to enter into a new Contract
- Assignment
- Third Party Rights
- Governing Law
- This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.]

Guarantor company	[Enter Company name] 'Guarantor'
Guarantor company address	[Enter Company address]
Account manager	[Enter Account Manager name]

	Address: [Enter Account Manager address]
	Phone: [Enter Account Manager phone number]
	Email: [Enter Account Manager email]
	Fax: [Enter Account Manager fax if applicable]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	Meaning
Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].

Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.
Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words ‘other’ and ‘otherwise’ are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

- reference to a gender includes the other gender and the neuter
- references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time
- any phrase introduced by the words ‘including’, ‘includes’, ‘in particular’, ‘for example’ or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

- fully perform or buy performance of the guaranteed obligations to the Buyer

- as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[Enter Address of the Guarantor in England and Wales]

[Enter Email address of the Guarantor representative] For

the Attention of [insert details]

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

- delivered by hand, at the time of delivery
- posted, at 10am on the second Working Day after it was put into the post

- sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

- any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
- any amendment to or termination of the Call-Off Contract
- any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
- the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

- it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee
- it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person
- if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor
- the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

- obtain judgment against the Supplier or the Guarantor or any third party in any court
- make or file any claim in a bankruptcy or liquidation of the Supplier or any third party
- take any action against the Supplier or the Guarantor or any third party
- resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer's rights may be exercised as often as the Buyer deems expedient. Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

- the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation
- has the capacity to sue or be sued in its own name
- the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets
- the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee
- the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:
    - the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgment, decree or permit to which the Guarantor is subject
    - the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets
    - all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that

the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor's acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of Guarantee by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers [enter the Supplier name] [or a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [insert fax number] from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[Insert name of the Guarantor] acting by [Insert names]

Director

Director/Secretary

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	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.

Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.

Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives 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	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.

Data Subject	Takes the meaning given in the UK GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
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-todate 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.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).

Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.

UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.

Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

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

Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less

Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	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, judgment 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, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.

Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement 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.

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	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.

Protective Measures	Appropriate technical and organisational measures which may include: 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.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agiledelivery/spend-controlsche ck-if-you-need-approval-to-spendmoney-on-a-service

Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.

Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).

Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

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: Stephen Jones dpo@cabinetoffice.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are: Arul@fourseals.co.uk

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

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

Description	Details

Identity of Controller for each Category of Personal Data	The Buyer is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below ● Data (personal and sensitive) within Service Desk tooling provided by the Supplier ● Data (personal and sensitive) within correspondence between the Buyer and Supplier ● Data (personal and sensitive) residing within the COLA service as part of the operation of the service ● Any other Personal Data processed in order to deliver the Services

Duration of the Processing	Duration of the Call Off Contract, including any Extension Period
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this Call Off Contract
Type of Personal Data	Examples include, but are not limited to, names, email addresses, telephone numbers
Categories of Data Subject	Examples include, but are not limited to, Buyer's Staff, Supplier's Staff
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All relevant data to be deleted as soon as reasonably practical following completion of Processing, but in any event within 1 year after the expiry or termination of this Call Off Contract

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

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

Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

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

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

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

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

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

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [select: Supplier's or Buyer's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

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

2. Undertakings of both Parties

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

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

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

3. Data Protection Breach

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

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

(b) all reasonable assistance, including:

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

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

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

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data

Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

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

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

4. Audit

4.1 The Supplier shall permit:

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

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

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

5. Impact Assessments

5.1 The Parties shall:

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

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

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

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

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

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

(b) if in the view of the Information Commissioner, the Supplier is responsible for thePersonal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors,

on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner,then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In

the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

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

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

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

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

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

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

8. Termination

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

9. Sub-Processing

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

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

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

10. Data Retention

10.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy