



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	2
Part B: Terms and conditions	15
Schedule 1: Services	36
Schedule 2: Call-Off Contract charges	37
Schedule 3: Collaboration agreement	38
Schedule 4: Alternative clauses	51
Schedule 5: Guarantee	56
Schedule 6: Glossary and interpretations	65
Schedule 7: UK GDPR Information	83
Annex 1: Processing Personal Data	84
Annex 2: Joint Controller Agreement	89
Appendix 1 – Unily SLA	93

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	849972571223081
Call-Off Contract reference	
Call-Off Contract title	UKHSA Pulse Intranet Service
Call-Off Contract description	Provision and hosting of UKHSA Pulse Intranet
Start date	01/01/23
Expiry date	31/12/25
Call-Off Contract value	£449,030.77
Charging method	Invoiced annually in advance
Purchase order number	TBC

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

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

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

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

<div>From the Buyer</div>	<div>UKHSA</div> <div></div> <div></div> <div></div> <div></div>
<div>To the Supplier</div>	<div>Unily Limited</div> <div></div> <div></div> <div></div> <div></div> <div></div>
<div>Together the ‘Parties’</div>	

Principal contact details

For the Buyer:

Name: [REDACTED]

Email: [REDACTED]

For the Supplier:

Name: [REDACTED]

Email: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01/01/23 and is valid for 36 months
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 90 days from the date of written notice for Ending without cause (as per clause 18.1). The Buyer acknowledges that the Call-Off Contract Charges are non-cancellable, and any remainder of the Call-Off Contract Charges will become immediately due and payable in full should the Call-Off Contract be terminated for convenience as per this section.</p>

Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 30 days written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p>https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</p>
-------------------------	--

Buyer contractual details

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

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 2: Cloud Software • Lot 3: Cloud Support
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <ul style="list-style-type: none"> • The Supplier will provide the Buyer with Support Services as set out under Support Service Level agreement section.
Additional Services	N/A
Location	The Services will be delivered remotely
Quality Standards	The quality standards required for this Call-Off Contract are in accordance with established technology and good industry standards and for overall Buyer satisfaction.
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are as detailed in the relevant Support Services level.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are: See Unily SLA – Appendix 1
Onboarding	The onboarding plan for this Call-Off Contract is N/A

Offboarding	<p>The offboarding plan for this Call-Off Contract is: Upon request by the Buyer made before or within 30 days after the effective date of termination, the Supplier will make available to and/or assist the Buyer with the ability to export and download all Buyer materials. For the avoidance of doubt, the Supplier will provide an export of the Buyer materials which includes images and documentation to the Microsoft Azure blob location.</p>
Collaboration agreement	N/A
Limit on Parties' liability	<p>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 in aggregate £500,000 per year</p> <p>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 £2,000,000 or 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of £1,000,000 or 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>

Insurance	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> • 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 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	<p>The Buyer is responsible for and acknowledges that:</p> <ol style="list-style-type: none"> 1. Buyer must all times use the Platform in accordance with the terms of the Agreement. 2. The Buyer acknowledges and agree that: <ol style="list-style-type: none"> a) Supplier is not itself providing hosting services, such services are provided by the Platform Provider b) The Agreement does not provide the Buyer with any independent right to use or access the Platform outside the scope of this Agreement. 3. The Access Services: <p>Buyer's access and use of the Services and the license granted by the Supplier to the Buyer under is subject to the following conditions and limitations:</p> <ol style="list-style-type: none"> (a) Only users with Office 365 will be able to utilise out of box integration with Office 365; (b) Buyer must ensure that all Authorised Users of the Services comply with the terms of the Agreement and any relevant third-party terms applicable to the use of the Platform; (c) Buyer must not use and must ensure the Services are not used: <ol style="list-style-type: none"> i. in any way that causes, or may cause, damage to the Platform or impairment of the availability or accessibility of the Platform, or any of the areas of, or services on, the Platform (other than through the normal course of use); and ii. in any way that is, or in connection with any purpose that is unlawful, illegal, fraudulent or harmful. (d) Buyer shall:

	<p>i. not sub-license, transfer or loan the Application or otherwise make it available to or use it to provide services to any third party except and Affiliate or a sub-contractor; and</p> <p>ii. ensure that Authorised Users' access codes are kept secure and confidential;</p> <p>iii. ensure that each User Licence is not used by more than one individual (however user licenses may be transferred from an Authorised User to another individual on a permanent basis);</p> <p>iv. procure the Authorised Users' compliance with the terms of this Agreement and the Documentation; and</p> <p>v. not make any copies of, disseminate or use the Documentation or any part of it in any way except for as permitted under the Agreement.</p> <p>For the avoidance of doubt, the Buyer has no right to access the object code or source code of the Application, either during or after the expiry or termination of the Agreement, and the Buyer must not reverse engineer or seek any access to the whole or any part of the Application.</p> <p>(e) Buyer shall be solely responsible for:</p> <p>i. procuring and maintaining its network connections and telecommunications links from its systems to the Application; and</p> <p>ii. all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to Buyer's network connections or telecommunications links or caused by the internet.</p> <p>The Supplier is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Buyer acknowledges that the Services may be subject to limitations, delays and other problems inherent in the use of such communications facilities.</p>
Buyer's equipment	<p>The Buyer's equipment to be used with this Call-Off Contract includes – N/A</p>


Supplier’s information

Subcontractors or partners	<p>The following is a list of the Supplier’s Subcontractors or Partners:</p> <p>Sub-processing covered in Schedule 7</p>
-----------------------------------	---

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	<p>The payment method for this Call-Off Contract is BACS</p>
Payment profile	<p>The payment profile for this Call-Off Contract is annually in advance.</p>
Invoice details	<p>The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.</p>
Who and where to send invoices to	<p>Invoices will be sent to [REDACTED] and then reviewed prior to forwarding to accounts payable.</p>

Invoice information required	All invoices must include UKHSA's PO number which will be provided upon contract signature.
Invoice frequency	Invoice will be sent to the Buyer annually.
Call-Off Contract value	The total value of this Call-Off Contract is £449,030.77
Call-Off Contract charges	

Additional Buyer terms

Performance of the Service	N/A
-----------------------------------	-----

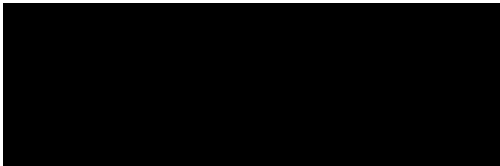
Guarantee	N/A
Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	N/A
Alternative clauses	N/A

Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>Title: Unily Exit Plan and Additional Exit Plan relating to UKHSA's Call-Off Contract for the provision and hosting of UKHSA Pulse Intranet.</p> <p>Upon termination or expiration of the Call-Off Contract, the Supplier will provide an export of the SQL database storing all Unily content (Stories, etc.) which contains all data and metadata in a structured data format. This database backup (bacpac file) can be restored to SQL and queried to retrieve all necessary data. In addition to this, an export of the blob storage, which contains all images and documents uploaded to Unily, will be provided in a compressed file format (such as zip file). This can be decompressed and all images, documents can be retrieved.</p> <p>Neither of these items (database backup and blob storage export) will be encrypted. A database administrator with SQL querying skills combined with an individual who has knowledge of Unily's content management system will be able to retrieve the required content. This content can then be re-factored or transformed to be prepared for import to another content management system as required by the Buyer.</p>
Personal Data and Data Subjects	<p>Personal data is being processed for the provision of the Services and therefore, Schedule 7 is used. The Controller to Processor data protection clauses set out in Schedule 7 of the Framework Agreement (which is incorporated into this Call-Off Contract) are reproduced at Schedule 7 as amended in accordance with PPN 03/22.</p>
Intellectual Property	<p>Note any Project Specific IPR that may arise and require assignment and otherwise note any other required amendments to standard IPR provisions.</p>

Social Value	N/A
---------------------	-----

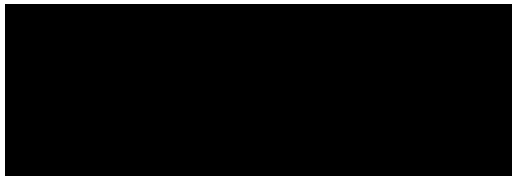
1. **Formation of contract**
- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.
2. **Background to the agreement**
- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed for and on behalf of the supplier:



Full Name: [Redacted]
Job Title/Role: Global Head of Contracts
Date Signed: 19 July 2023

Signed for and on behalf of the buyer:



Full Name:



Job Title/Role: Head of Category, Digital & Technology

Date Signed: 19/07/2023

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) (and Schedule 7 (Processing Data))
- 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

2.2.4 Schedule 7 (Processing Data) has been amended in accordance with PPN 03/22.

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 extend existing policies bought under the Framework Agreement. Such additional insurance policies will be at the Supplier's sole discretion. Any request shall not be unreasonably refused or delayed

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-securityclassifications>
- 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-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/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, and subject to the parties' agreement 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. The expenses of such diligence shall be borne solely by the Buyer. After both parties' agreement of 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 (which are subject to the Supplier's review) 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

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 Where applicable, 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 back to the Buyer 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, where required and requested by the Buyer, the Supplier must maintain an up to date exit plan also referred to as additional exit plan during the extended Call-Off Contract Term.
- 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 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 its chosen replacement supplier upon receipt of the Buyer's Data from the existing 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, 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

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

21.9 For the purpose of this Clause 21, the Supplier's exit plan and additional exit plan are as set out in the Order Form's Buyer specific amendments to/refinements of the Call-Off Contract terms section.

22. Handover to the buyer

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 and 29 shall be capped at the value of the contract. Clause 11 shall be unlimited.

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 Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services



UKHSA -Existing
Features and Function

Embedded below:

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:

	Year 1 1/1/2023 to 31/12/2023	Year 2 1/1/2024 to 31/12/2024	Year 3 1/1/2025 to 31/12/2025	Total
Users				
Evergreen Module				£449,040.00
Total				£449,040.00
Grand Total				£449,040.00
Price Per User License / Year				
Price Per User License / Month				
Grand Total				£449,040.00

Schedule 3: Collaboration agreement - Not used

Schedule 4: Alternative clauses - Not Used

Schedule 5: Guarantee – Not Used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Business Hours	Between 08:00 and 18:00 on any weekday, other than a bank or public holiday, in England.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.

Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.

Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none">• information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	<p>'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.</p>
Controller	<p>Takes the meaning given in the UK GDPR.</p>
Crown	<p>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.</p>
Data Loss Event	<p>Event that results in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.</p>

Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')
End	Means to terminate; and Ended and Ending are construed accordingly.

Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force <p>Majeure at the time this Call-Off Contract was entered into</p> <ul style="list-style-type: none"> • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	<p>A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.13 together with the Framework Schedules.</p>

Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
--------------	---

	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • 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	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, 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, provided that Losses do not include any losses suffered by the Buyer or any third party for (a) any direct or indirect loss of or damage to profit or reputation, or (b) for any indirect or consequential loss or damage of any kind or for any loss or damage suffered as a result of a claim brought by any third party; or (c) any loss or corruption of any Buyer Data within the Buyer's platform, database or other software except for any such loss or corruption arising from the Supplier's negligence or intentional or wilful misconduct.

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 Unily tenant on the Microsoft Azure platform hosting the Application.
Platform Provider	The person, or entity, contractually responsible for making the Platform available to Supplier, whether Microsoft or its authorized reseller, or a third party acting for and on behalf of Supplier such as a provider of a private cloud)
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none">• induce that person to perform improperly a relevant function or activity• reward that person for improper performance of a relevant function or activity• commit any offence:<ul style="list-style-type: none">○ under the Bribery Act 2010○ under legislation creating offences concerning Fraud○ at common Law concerning Fraud○ committing or attempting or conspiring to commit Fraud
-----------------------	---

Project Specific IPRs	<p>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.</p>
Property	<p>Assets and property including technical infrastructure, IPRs and equipment.</p>
Protective Measures	<p>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.</p>

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 – Refer to Schedule 1 insert/attachment
Service description	The description of the Supplier service offering as published on the Platform.

Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.

Sub processor	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: Processing Data

This schedule reproduces the annexes to schedule 7 (Processing Data) 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.

Schedule 7 Annex 1 – Part 1 – Controller to Processor Clauses

1. Data Protection

1.1 The Parties acknowledge that for the purposes of Data Protection Legislation, the Buyer is the Controller, and the Supplier is the Processor. The only processing that the Processor is authorised to do is listed in Schedule 7, Annex 1 – Part 2 by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR.

1.1.1 The Buyer warrants and represents that the Supplier's expected use of the Buyer Personal Data for the delivery of the Services and as specifically instructed by the Buyer will comply with the Data Protection Legislation. 1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe Data Protection Legislation.

1.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, taking into account the nature of Processing and information available to the Processor, include:

- i. a systematic description of the envisaged processing operations and the purpose of the processing.

- ii. an assessment of the necessity and proportionality of the processing operations in relation to the Services.
- iii. an assessment of the risks to the rights and freedoms of Data Subjects; and
- iv. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

- a) process that Personal Data only in accordance with this Schedule 7, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor will use commercially reasonable efforts to propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:

- (i) nature of the data to be protected;
- i.(ii) harm that might result from a Data Loss Event;
- ii.(iii) state of technological development; and
- iii.(iv) cost of implementing any measures;
- b.c) ensure that:
 - i.(i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 7);
 - ii.(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this clause;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
 - (E) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained, such consent is given by the Buyer for Supplier to transfer Personal Data to the appointed Subcontractors and new Subcontractors pursuant to clauses 1.15 and 1.6, and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
 - (ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor complies with its obligations under Data Protection Legislation by providing an appropriate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - d.(v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
 - e.e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

- 1.3 1.5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:
- a.a) receives a Data Subject Request (or purported Data Subject Request);
 - b.b) receives a request to rectify, block or erase any Personal Data;
 - c.c) receives any other request, complaint or communication relating to either Party's obligations under Data Protection Legislation;
 - d.d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
 - e.e) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- 1.4f) becomes aware of a Data Loss Event.
- 1.6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Data Loss Event;
- 1.6(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

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

- (a) the Controller determines that the processing is not occasional;
 - (b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
- (a)(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Processor shall allow for audits of its Personal Data processing activity by the Controller or the Controller's designated auditor (subject to reasonable and appropriate confidentiality undertakings), providing that neither the Controller nor any designated auditor(s) shall have access to any data and Personal Data from the Processor's other customers or to systems or facilities not involved in processing the Buyer Personal Data under this schedule 7.

1.10 The Controller agrees that where it decides to exercise its audit rights in Clause 1.9, it shall:

- (a) prior to requesting an inspection or audit pursuant to Clause 1.9, take into account the relevant third-party certifications and audits already applicable to the Processor; and
- (b) give the Processor reasonable written notice, at least 60' Business Days in advance, of any assistance, information, and co-operation request and any request to conduct an audit or inspection under Clause 1.9 within Business Hours, and will take (and ensure that its designated auditor(s) takes) reasonable measures to avoid and prevent any damage or injury and minimise any disruption from such audit or inspection.

1.11 An audit will be conducted no more than once annually during the term of the Framework Agreement, except where required by the Information Commissioner's Office or Data Protection Legislation.

1.12 The Controller shall bear the full costs of any such audits and inspections and shall

reimburse the Processor for reasonable costs and expenses incurred by the Processor pursuant to such audits and inspections, including any time expended by the Processor, its Affiliates or its Subprocessors for any such audits or inspections at the Processor's then-current services rates, which shall be made available to the Controller upon request.

1.13 Each Party shall designate its own Data Protection Officer if required by Data Protection Legislation.

1.14 Other than those Sub processors listed in Schedule 7 Annex 1 – Part 2 (**Approved Sub processors**) and subject to clause 1.15, the Processor shall not authorise any other third party or Sub processor to process the Buyer Personal Data.

1.15 The Controller expressly consents to the Supplier's engagement of new Sub processors (each a "**New Sub processor**") subject to the terms set forth in this clause 1.15 and 1.16. The Processor shall provide the Controller with a mechanism to subscribe to updates to the Sub processor list, to which the Controller shall subscribe, and the Processor shall provide such updates at least thirty (30) days before any New Sub-processor(s) process the Buyer Personal Data to any other person (including any Subcontractors) for the provision of the Services.

1.16 If the Controller does not object in writing to the appointment of a New Sub processor (on reasonable grounds relating to the protection of Buyer Personal Data) within ten (10) days of the Supplier adding that New Sub processor to the Processor's Sub processor List, the Controller agrees that it will be deemed to have authorised that New Sub processor. If the Controller provides such a written objection to the Processor, the Processor will notify the Controller in writing within 30 days that either: (a) a commercially reasonable change to the Controller's configuration or use of the affected Services to avoid processing of Buyer Personal Data by the objected-to New Sub processor can be made; or (b) that the Processor is unable to make available such change. If the notification in paragraph (b) is given, in particular where the Controller objects to any Sub processor that is essential to allow the Processor to provide the Services then, the Processor shall terminate the Call-Off Contract in writing within 30 days' written notice.

Before allowing any Sub processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub processor and processing in accordance with the terms set forth in clause 1.15;

(b) enter into a written agreement with the Sub processor which give effect to the terms set out in this Schedule 7 such that they apply to the Sub processor; and

(c) provide the Controller with such information regarding the Sub processor as the Controller may reasonably require.

1.17 The Processor shall remain fully liable for all acts or omissions of any of its Sub processors.

1.18 The Parties agree to take account of and comply with any guidance issued by the Information Commissioner's Office and where such guidance requires or merits changes to the Call-Off Contract (including this Schedule 7), the Parties shall use reasonable endeavours to enter into a Variation (in accordance with clause 32) within 30 working days of such guidance being issued.

Schedule 7 Annex 1 – Part 2: Schedule of Processing, Personal Data and Data Subjects

This Annex 1 – Part 2 shall be completed by the Controller, who may take account of the view of the Processor, however, the final decision as to the content of this Annex 1 – Part 2 shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are:

[REDACTED]



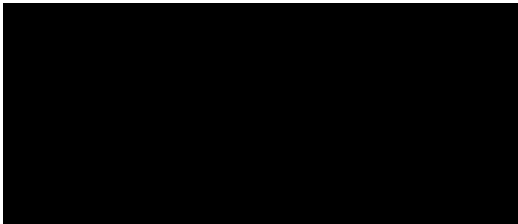
1.2 The contact details [REDACTED]
[REDACTED]

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

1.4 Any such further instructions shall be incorporated into this Annex 1 – Part 2.

Description	Details
Identity of Controller for each Category of Personal Data	The Parties acknowledge that for the purposes of Data Protection Legislation, the Buyer is the Controller, and the Supplier is the Processor in accordance with Clause 1.1.

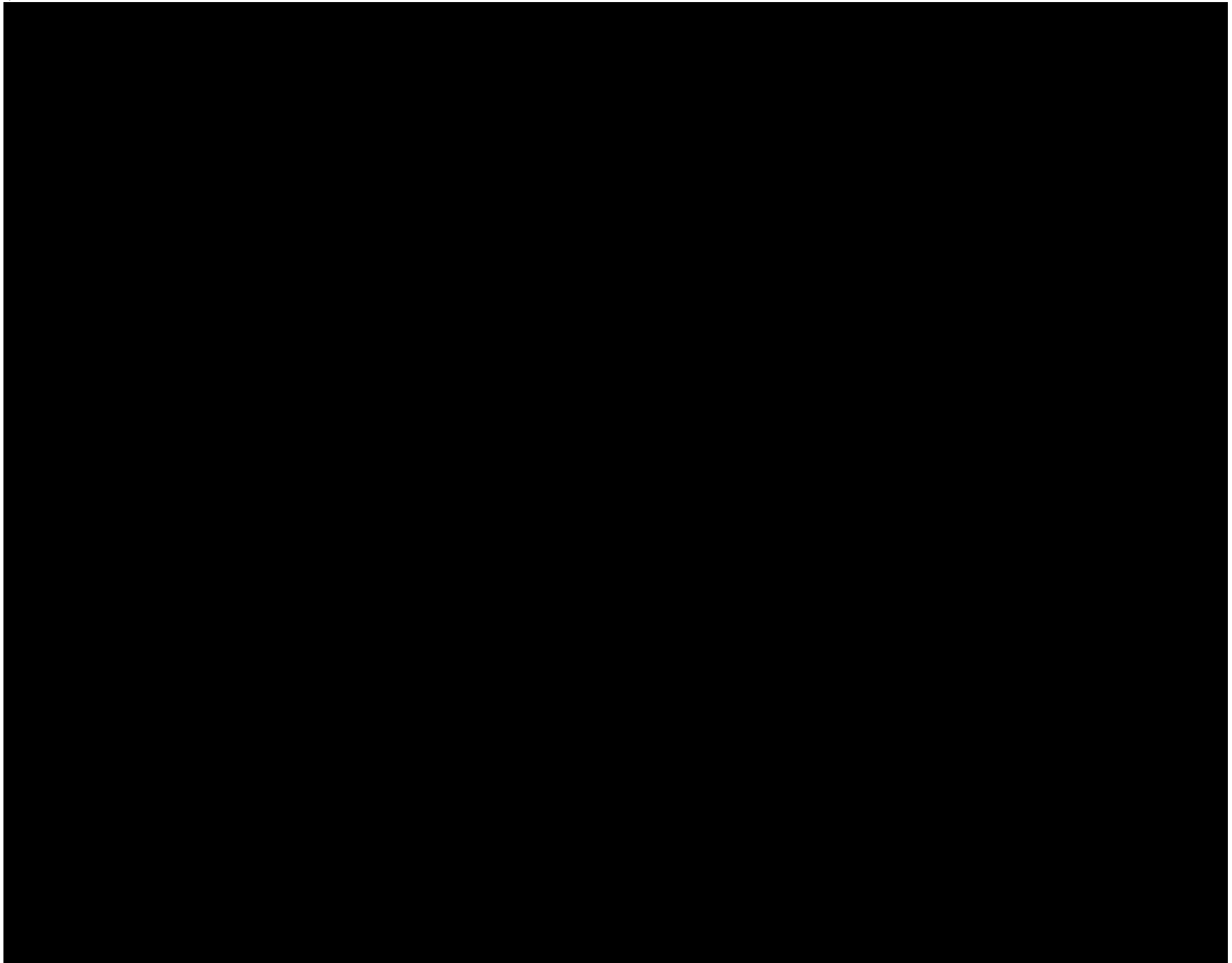
<i>Subject matter of the processing</i>	All Personal data processed by the Supplier is in a business/commercial and/or employee context (on the behalf of the employer) as a supplier.
Duration of the Processing	Term of the contract – 01/01/23 – 31/12/25
Nature and purposes of the Processing	To provide the Buyer with the Services. To provide the Buyer with an employee experience intranet platform and other related Services as described in the Framework Agreement. The Unily platform is an internal employee facing intranet and it is not intended to be used or aimed at consumers/individuals not acting in employment or commercial contexts. All Personal data processed by the Supplier is in a business/commercial and/or employee context (on the behalf of the employer) as a supplier.
Type of Personal Data being Processed	<ul style="list-style-type: none"> • Personal details (name, date of birth, age, job title, users, work email, work phone, work mobile, job title, department, location, IP address, browser agent, device type, profile image, twitterID, LinkedInID, userID) • Contact details (address, email and telephone number etc.) • Information technology data such as IP address, browser agent, device type or where a website accessed from • Analytics data, including platform usage and content consumption. • And any other types of Buyer Data which may be provided by Buyer from time to time via data synchronization process to facilitate customized functions and integrations with third party applications.

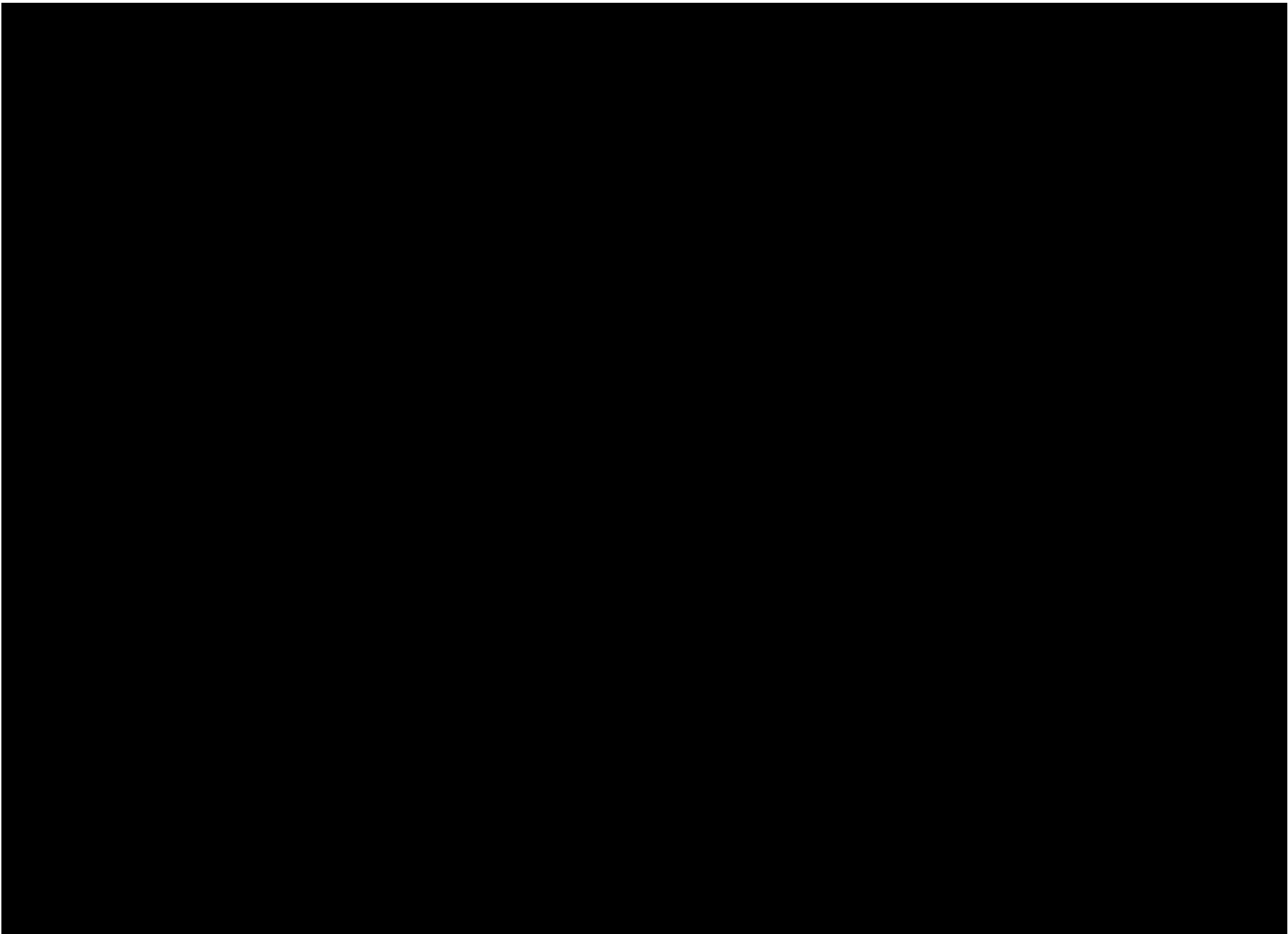
Categories of Data Subject	<p>Includes:</p> <ul style="list-style-type: none">i. CSS staff concerned with management of the Framework Agreementii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreementiii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Agreementiv. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Agreementv. Buyer Personnel
Controller privacy notice	

<p>International transfers and legal gateway</p>	<p>Buyer Personal Data is stored within a Microsoft Azure data centre in the same legal boundary as the Buyer's Office 365/Azure Active Directory tenant. Additionally, disaster recovery copies of the data is geo-replicated to a Microsoft Azure datacentre within the same judicial data boundary.</p> <p>All Buyer Personal Data is stored on Microsoft Azure SQL databases with Transparent Data Encryption 256 bit AES, and Microsoft Azure Storage Accounts with Storage Encryption 256 bit AES. Keys are managed by Microsoft.</p> <p>In addition, the Supplier's Approved Sub-processors will process Buyer Personal Data (see below). The Supplier ensures transfers to Approved Sub processors are in accordance with the Data Protection Legislation (including where applicable completing a transfer risk assessment and data processing addendum/international data transfer agreement)</p>
<p>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</p>	<p>All Buyer Personal Data to be deleted after the expiry or termination of this Agreement unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder.</p>
<p>Approved Sub processors</p>	<p>See list below.</p>

Third party sub-processors

DocuSign Envelope ID: EC2EF6AE-31AE-4728-9048-E73F32D043CA





Schedule 7 Annex 2: Security

External Certifications The Supplier shall hold at least Cyber Essentials Plus certification (or an equivalent) and ISO 27001:2013 certification.

Risk Assessment The Supplier shall perform a technical information risk assessment on the Services supplied and be able to demonstrate what controls are in place to address those risks.

Security Classification of Information The Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that information classified as OFFICIAL, OFFICIAL-SENSITIVE and/or Personal Data is safeguarded in accordance with the applicable legislative and regulatory obligations.

End User Devices

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

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

Testing The Supplier shall at its own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Buyer data being transferred into its systems. The ITHC scope must be agreed with the Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Buyer data.

Networking The Supplier shall ensure that any Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

Personnel Security All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Supplier may be required to implement additional security vetting for some roles.

Identity, Authentication and Access Control The Supplier must operate an appropriate access control regime to ensure that users and administrators of the Services are uniquely identified. The Supplier must retain records of access to the physical sites and to the Services.

Data Destruction/Deletion The Supplier must be able to demonstrate it can supply a copy of all data on request or at termination of the Services, and must be able to securely erase or destroy all data and media that the Buyer Data has been stored and processed on.

Audit and Protective Monitoring The Supplier shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Buyer Data. The retention periods for audit records and event logs must be agreed with the Buyer and documented.

Vulnerabilities and Corrective Action The Supplier shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

The Supplier must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

Secure Architecture The Supplier shall design the service in accordance with:

- NCSC "[Secure design principles - NCSC.GOV.UK](#)"
- NCSC "[Protecting bulk personal data - NCSC.GOV.UK](#)"
- NSCS " [The cloud security principles - NCSC.GOV.UK](#)"

Appendix 1 – Unily SLA

The service level and availability criteria required for this Call-Off Contract are

1 DEFINITIONS. As used below:

1.1 In this Agreement, unless the context otherwise requires:

“Acknowledged” means an acknowledgment of the Receipt either by Support Portal, phone or email;

“Agreed Service Time” or “AST”

means the availability of the Application, which shall be twenty-four (24) hours a day, seven (7) days a week, and three-hundred and sixty-five (365) days a year excluding Scheduled Maintenance, Emergency Maintenance outages, and any issues outside of Supplier’s control;

“Application” means the intranet software application called “Unily” comprised of the Modules;

“Business Day” also known as Working Hours means any weekday, other than a bank or public holiday in England;

“Business Hours” means between 08:00 and 18:00 on a Business Day;

“Change Management Process” means controls of the lifecycle of all configuration items, enabling beneficial changes to be made with minimum disruption to IT services;

“Change Request” means the addition, modification, or removal of anything that could affect production environment;

“Commissioners” means the representatives nominated by the Buyer during the implementation stage and listed by the Supplier as individuals who will be responsible for initiating the Support Services request;

“Emergency Maintenance” means a period of time during which the Application is not available because the Supplier needs to implement a response to an emergency outside of its control (for the avoidance of doubt, shall include “Emergency Maintenance” or “Emergency Patch”);

“Incident” means an unplanned interruption to an Application performance or reduction in the quality of the production environment as opposed to a Service Request which is defined as formal request from the Buyer for support to be provided;

“Incident Management (IM)” means the process responsible for managing the lifecycle of all Incidents. Incident Management ensures that normal Application performance is restored as quickly as possible and business impact is minimised;

“Level 1 Support” means the first team to engage with any Incidents reported by the Commissioner via IT Services Management (ITSM);

“Major Incident Report” or “MIR” means the review which documents initial underlying causes (if known), complete resolution history, and identifies next steps or internal opportunities for improving the handling of future major Incidents;

“Priority 1” Incident or “P1” means the Application is unavailable or significant reduction or degradation in Application performance, affecting all or multiple users;

“Priority 2” Incident or “P2” means a reduction or degradation of Application performance affecting multiple users;

“Priority 3” Incident or “P3” means a reduction or degradation of Application performance affecting an individual or a small set of local individual users;

“Priority 4” Incident or “P4” means an Incident affecting a single user, including an unexpected error or response from the Application;

“Priority Level” means the level of priority of an Incident, whereby Priority 1 is the highest priority level and Priority 4 is the lowest priority level;

“Problem” means a cause or potential cause, of a single significant Incident, multiple recurring Incidents or representation of the potential cause of one or more outages;

“Problem Management Process” means an IT service management process that handles reactive and proactive problems. This process minimises the impact of recurring incidents, and strives to identify and resolve the root cause of problems as well as proactively detect and address potential incidents, so that incidents can be prevented or mitigated;

“Product Bug” or “Bug” means the cause of the reported Incident has been identified as an issue with the core Application code and will need a new release or a hotfix to resolve. The Product Bug could have materially adverse effects on the appearance, operations, or functionality of the Application;

“Product Bug Process” means the process where a reproducible Product Bug (stemming from an Incident or Problem) is identified and investigated through a development sprint cycle, and the fix or resolution of such bug is released through an updated version of the Application;

“Project Team” means the designated team of experts to assist on the project through to go-live;

“Receipt” means the receipt by the Supplier of a message via Support Portal, phone or email from a Commissioner regarding an Incident;

"Recovery Time Objective or RTO" means the maximum amount of time to recover the Application to a fully functional state;

"Recovery Point Objective or RPO" means the maximum amount of time that data loss is permissible;

“Response” means a result in one of the following:

- A fix to an Incident or completion of a service request;
- A recommendation to implement a temporary workaround;
- A request for further information regarding the problem or further investigative procedures to be carried out by a Commissioner; or
- A status update was provided by the Supplier to the Buyer on the progress of the Incident.

“Scheduled Maintenance” means a period of time during which the Parties have previously agreed (in accordance with the Agreement or otherwise) that a Service will not be available (which for the avoidance of doubt, shall include “Scheduled Maintenance” or scheduled “Patching”);

“Service Levels” means the required level of service;

“Service Request” means a request for such things as data export requests or planned event/announcement, account creation or any other request by the Buyer and which is not an Incident. The SLAs set for completions of Service Requests can vary but are aimed to be completed within seven (7) Business Days, which commences after submissions and approval by the Supplier of the Service Request in Support Portal;

“Support Portal” means Supplier Support Services’ IT services management online portal where Commissioners can log Incidents;

“Support Service” means a service provided by the Supplier in respect of the Application with the aim of resolving any Incident of the Application and maintaining the Application fully operational under Clause 2.3 of this Schedule; and

“Unscheduled Maintenance” mean a period of time during which the Service is not available, and which is not a Scheduled Maintenance or Emergency Maintenance

2 SUPPORT SERVICES

2.1 The Supplier undertakes to provide the Buyer with Support Services remotely in respect of the Application.

2.2 Any amendments to the Support Services must be agreed upon between the Parties in writing.

2.3 The Support Services shall comprise the following:

2.3.1 Advisory and remote support to the Application

(a) During Business Hours, the Supplier shall provide consultancy and systems analysis in relation to the Application to enable the Buyer to:

(i) obtain the best possible use of the Application; and

(ii) resolve any difficulties it may have as to the use and/or operation of the Application.

(b) The Supplier shall provide diagnostic assistance to the Buyer by email to diagnose and correct Incidents remotely.

2.3.2 All Incident Correction

(a) All communication reporting an Incident by a Commissioner will be recorded by the Supplier in ServiceNow and given a unique number for audit and tracking purposes. The unique tracking number for each report logged will be emailed to a Commissioner within one (1) hour of entry on the database. This is deemed to be an Acknowledged response.

(b) All Incidents will be assigned a Priority Level depending on the critical urgency at the point of notification of the Incident by a Commissioner.

(c) the Supplier will endeavour to provide support and/or correct Incidents as soon as reasonably possible to meet the business needs of a Commissioner where the resolution is within the control of the Supplier.

(d) The Supplier shall obtain the approval of a Commissioner before implementing any proposed changes arising out of the correction of a reported Incident (such as having to take down Buyer's site temporarily).

(e) The Supplier does not guarantee that it can resolve all Incidents. In some circumstances (such as where modifications have been made to the Application without the Supplier's prior written consent), the Supplier may be unable to provide a satisfactory Incident resolution.

3 APPLICATION SUPPORT SERVICE EXCLUSIONS

3.1 The Support Services to be provided shall not include the correction of any defects or errors found in or resulting from Buyer's operating system, hardware or network, or any other software or code not provided by the Supplier.

3.2 Upon request by the Buyer, the Supplier shall provide additional Support Services to try to remedy defects, bugs or errors caused by any of the factors listed in clause 3.1.

3.3 For the avoidance of doubt, the Supplier will not be responsible for fixing any errors, bugs or viruses which are inherent in Microsoft Office 365 or other Buyer's third-party software, that is not provided or made available by the Supplier.

4 SUPPLIER'S RESPONSIBILITIES

The Supplier shall ensure that:

4.1 it shall perform the Services with reasonable skill, care and diligence;

4.2 the Services shall be performed in accordance with good industry standards and practice;

4.3 it shall communicate in writing any outages/infrastructure changes with the possible impact on Buyer's use of the Application;

4.4 it shall use reasonable endeavours to minimise the interruption to Buyer's business by the provision of Services; and

4.5 it shall provide suitably qualified, experienced, and trained personnel to carry out the Services or related tasks.

5 BUYER'S OBLIGATIONS

5.1 Throughout the Term of the Principal Agreement, Buyer shall afford the Supplier and/or any of its personnel such access to the Application as may be reasonably necessary for the proper performance of the Services. In addition, the Buyer shall:

5.1.1 make available any Buyer's representatives who may be required by the Supplier to resolve the Incident;

5.1.2 communicate any changes to system configuration or usage;

5.1.3 specify the members of staff who can make use of the Support Services. The Supplier will not provide Support Services to any individuals who are not listed as Commissioners;

5.1.4 in accordance with clause 10.5 below, supply all documentation and other information necessary for the Supplier to diagnose any Incidents or bugs in the Application; and

5.1.5 copy and use any modifications, corrections, or enhancements to the Application delivered to it hereunder only in accordance with the applicable license conditions granted for the Application.

6 SCHEDULED OUTAGE AND EMERGENCY OUTAGES

6.1 The Supplier will have up to two (2) Scheduled Maintenance windows per annum. Each downtime window is scheduled between 18:00 pm Friday to 06:00 am Monday (London, UK local time). The precise times and dates for this downtime will be communicated by the Supplier at least fourteen (14) days in advance of any Scheduled Maintenance.

6.2 In the event any Scheduled Maintenance or Patching requires downtime to be extended, the Supplier will advise the Buyer and provide regular updates until the Application performance resumes. Any unplanned extension to Scheduled Maintenance or Patching downtime will be considered Unscheduled Maintenance time.

6.3Emergency Maintenance and Patching may be required (but not limited) to protect against imminent threats. Where reasonably practicable, an Emergency Maintenance or Emergency Patching downtime will be planned outside of Business Hours and with two (2) days’ advanced notice provided to the Buyer. For the avoidance of doubt, such notice period will depend on the extent of the critical urgency.

7 CHANGE MANAGEMENT

7.1The Supplier has defined and developed a Change Management Process to understand and minimise the risks and negative impacts of changes to the production services, and to document and manage the scope and implementation of changes.

8 DEPLOYMENTS

8.1All release upgrades and deployments will be scheduled during Business Hours on Business Days between 09.00 am and 5:00 pm Monday to Thursday (London, UK local time). The Supplier will use its best endeavours to ensure that any disruption to the Services is kept to a minimum where a planned upgrade and /or deployment results in an extended period of downtime greater than the planned scheduled hours, the Supplier will continue to work to restore Services while providing regular updates.

8.2The Buyer will be required to stay within three (3) major versions of the Unily Application to continue to benefit from the latest platform capabilities, optimisations, and Support Services. Please note, if a critical or security risk is identified by the Supplier, this may prompt the Supplier to upgrade or deploy as part of the Emergency Change/Deployment process. The Supplier will communicate prior to this being actioned.

8.3For the avoidance of doubt, where a Buyer’s production site will require an outage, approval from the Buyer will be required in accordance with Supplier’s Change & Deployment Management practices.

9 ESCALATION MODEL

The following table outlines the responsible person(s) where Incidents communications are not received within pre-defined SLAs or Incidents are not managed to satisfaction:

Escalation

Type Business Escalations Technical Escalations

Day-to-day Assigned Customer Success Manager (CSM)

Level I Escalation

Assigned Customer Success Manager (CSM) Head of Customer Success

Support Manager,

EMEA APAC

Level II Escalation Head of Customer Success

Global Support Manager

Level III Escalation

Chief Customer Officer

Director of Technical Services

Requirements that are unsupported and/or referenced as out of scope (i.e., components that are managed by another vendor) are unable to be escalated. Such Incidents should be discussed within the Project Team.

10 INCIDENT MANAGEMENT PROCESS

10.1 Incidents are constantly monitored by the Supplier Support Services specialists.

10.2 Incidents are logged by Support Services specialists when emails are received, or the Commissioner can log directly via Support portal.

10.3 Incidents are prioritised based on an assessment of impact and urgency by the Support Services specialist. When an available Support Services specialist of the skill set is available, the ticket is updated where diagnostics and investigation are carried out. The Commissioner is contacted if further details are required.

10.4 Incidents are managed with the aim of restoring normal Application performance as soon as possible. Where Incidents appear complicated, and no mitigating or resolution steps are yet identified, Incidents are escalated to specialist teams for further investigation until resolution steps have been identified and implemented.

10.5 The Buyer is responsible for providing all relevant information and access to ensure an Incident can be investigated appropriately; failure to do this in a timely manner could result in the Incident not being resolved and potentially closed. If further information is required by the Support Services teams, the Buyer must provide this information within a commercially reasonable timeframe or risk the Incident being closed following requirements stated in the clause 10.6 below.

10.6 In the case that the Buyer fails to respond on three (3) separate occasions where the Supplier has requested information for troubleshooting purposes, the Incident will be updated and closed. Irrespective of the method of contact, the Supplier will try on three (3) separate days within a twenty-one (21)-day period and record communication attempts within the Incident record.

11 SERVICE LEVEL AGREEMENTS (“SLAs”)

Incident Management Communication SLAs*

Priority Communication SLAs

(For all incidents managed at Level 1 Support only) Communication hours/days when escalated to a specialist team such as development/product fix

P1 1 Hour 1 Hour

P2 2 Business Hours 8 Business Hours

P3 8 Business Hours 5 Business Days

P4 2 Business Days 10 Business Days

*The communication SLAs outlined above applies to Incidents only and are set to be communicated every ‘X’ Business Hours/Days (as described in the table above) until the Incident is resolved. This excludes Incidents that are identified as Product Bugs and follows a Product Bug Process cycle (as outlined under 11.2 and 11.3 below).

11.1 Please Note:

a) Major Incident Reports (“MIR”) will accompany all Priority 1 Incidents, which are to be submitted to the Buyer within twenty-four (24) hours of the Incident being resolved.

b) Internal problem investigations for the root cause analysis are not SLA bound and will follow Supplier Problem Management Process.

c) Where an MIR indicates issues outside of Supplier’s control, the Incident will be excluded from availability metrics (referenced under section 13).

d) If the Supplier requests information for troubleshooting purposes and the Buyer fails to respond on three (3) separate occasions, the Incident will be closed. For the avoidance of doubt, the Supplier must try on three separate (3) Business Days period and record this within the Incident record.

11.2 Product Bug Process:

A Product Bug fix will follow strict testing and release methodology before approval for release to customers and require a new deployment of the Application to the production instances and, if applicable, staging instance.

11.3 Identified Product Bugs (Usually 1-3 versions) resolution estimation:

a) Incidents tagged as product-specific Bugs will need to be aligned to new Application version releases.

b) Unify Application versions are released approximately every two (2) weeks.

c) The date the bug is identified will define the version to be released.

d) The complexity of the issue will define the release cycle where the Incident will be addressed.

e) Fixes will need to be applied to the production and, if applicable, staging. Deployment requests, scheduling, deployments and change controls will all need to be considered.

f) Hotfix solutions may be applied to critical-impact Incidents identified as product-specific Bugs in the Application. Applying a hotfix will be at the discretion of the Supplier Support Services team, operations, and product team.

11.4 Identified configuration Incidents (usually 0-4 weeks) resolution estimation:

a) Configuration Incidents can usually be directly addressed without the need for deployments, excluding third-party systems integration configurations.

b) For P1 Incidents, should the Application be unavailable due to a primary data center issue, the failover will automatically be triggered, and the Application will be hosted out of the secondary data center until such time as the primary is available again. There will be little to no derogation of the Application performance in this example.

c) If there are complications with the failover, where the secondary data center is unavailable or that the Incident is related to the Application, then a maintenance page will be displayed to anyone trying to access the site. This maintenance page can be branded and comprised of links to the critical line of business applications.

d) All P1 Incidents are managed twenty-four (24) hours a day, seven (7) days a week, with hourly communication as to the resolution progress.

12 AVAILABILITY AND AVAILABILITY OF SERVICE CREDITS

12.1 The Supplier commits to the Application being ninety-nine-point nine five percent of (99.95%) available during the Agreed Services Time. For the avoidance of doubt, availability should be calculated using the following method:

12.2 This is exclusive of any planned and agreed service outages.

12.3 Availability is measured automatically using the Supplier's monitoring services and calculated over each calendar month.

12.4 Upon request through the Support Portal, the Supplier will provide the Buyer with an uptime report in writing. The report will show the availability percentage over each calendar month, up to and including the last full calendar month, specific details of any outages including the date, and length of the outage and the cause where this was identified.

12.5 Without prejudice to any other rights and remedies of the Buyer, the Buyer shall be entitled to the following service credit if the monthly Availability percentage of 99.5% or more has not been achieved in any month:

AvailabilityService Credits

< 99.5% monthly uptime 3% refund of Access Charges in the preceding month

< 99.% monthly uptime 5% refund of Access Charges in the preceding month

< 98% monthly uptime 10% refund of Access Charges in the preceding month

12.6 In no event will the Availability Service Credit be greater than ten percent (10.00%) of the then current monthly Access Charges. The Buyer is responsible for providing the Supplier with accurate and up-to-date contact information for Buyer's designated points of contact. The Supplier will not be liable for any response times not met if the contact information provided by the Buyer is out of date or inaccurate, and the incorrect contact information is the cause of the failure to meet the response times.

12.7 Exclusions

Availability and Response Time measurements do not include periods of outages or non-response as a result of the following:

- Any act or omission on the part of the Buyer in violation of its obligations under the Agreement;
- Buyer's applications, equipment or facilities;
- Availability of Buyer's Microsoft 365 tenant;
- Resolution of Incidents related to the Buyer's Microsoft 365 tenant;
- Incidents deemed as feature requests and/or change requests;
- Incidents deemed to require custom development or configuration; or
- The Supplier's or the Buyer's Scheduled Maintenance under the condition that maintenance activity has been notified forty-eight (48) hours in advance.

13 RESOLUTION

13.1 The Supplier Support Services team makes best efforts to resolve every Incident as soon as possible. The assigned Support Services team member will provide the Buyer with regular updates on the status of an open Incident and will remain accountable for that Incident until closure.

13.2 While the intention of the Support Services team is always to resolve Incidents as quickly as possible, the Supplier is unable to commit to resolution times, including but not limited to the following:

- Amount or accuracy of the information supplied in the original ticket
- Supplier's ability to replicate the Incident.

- Where the Incident stems from:
 - Infrastructure (including, servers, network, database, etc.)
 - Supplier Product-level Bug
 - Buyer-specific Bug
 - Buyer Identity provider issues (AzureAD, OKTA, Forgerock etc)
 - Buyer Productivity suite issues (MS365, Google)
 - Third-party integrations (Support Portal, Workday, Concur etc.)
 - Third-party issue related to:
 - Azure data centre Incidents and outages
 - Broad Microsoft 365 issues

13.3 Incident Resolution

- a) An Incident shall be deemed to be resolved when the Supplier technician has provided a fix that can reasonably be expected to remove the negative impact affecting the Commissioner or the Buyer.
- b) Resolution actions may include:
 - i. Communication of corrective action to the Commissioner;
 - ii. An architecture system restart, restore or replacement; and
 - iii. Creation of enhancement or Bug fixes.
- c) If a Product Bug fix or enhancement is created, the full resolution will follow the Product Bug process.
- d) Once an Incident is resolved, the Commissioner has up to seven (7) days to test and confirm that the resolution is effective.
- e) During the course of the investigation, if a new issue is found, a separate Incident request must be raised by a Commissioner.

13.4 Incident Closure

- a) Once the Commissioner has tested and confirmed the fix is effective, or once seven (7) days have passed (whichever comes sooner), the Incident will be closed.
- b) Once the Incident is closed, the same Incident cannot be reopened. A new Incident record must be created if the issue reoccurs.

13.5 Disaster Recovery

The Supplier has a written disaster recovery plan in place ("DR Plan") which is tested annually to confirm that it will meet RTOs and RPOs. Unless specified elsewhere in the Agreement, the DR Plan includes an RTO of no more than twelve (12) hours and an RPO of no more than one (1) hour. Upon either Party's determination of a disaster that may impact the Services, such Party will promptly notify the other Party and the Supplier will (a) implement the DR Plan and (b) provide daily updates on the status of the Disaster Recovery progress. If the Services are impacted by a disaster, the Supplier will provide a post-mortem report detailing all actions taken by the Supplier to restore the Services.

13.6 Business Continuity

The Supplier has a written business continuity plan in place ("BC Plan"), which is designed to allow the Supplier to continue providing all Services under the Agreement without any material interruption in the event of a business disruption and to continue operating all Supplier business units or facilities that provide the Services.