Crown Commercial Service

G-Cloud 11 Call-Off Contract (version 4)

Contents

Part A - Order Form

Digital Marketplace service ID number:	146683211559092
Call-Off Contract reference:	FS430486
Call-Off Contract title:	Digital Asset Management System
Call-Off Contract description:	Digital Asset Management System
Start date:	31st March 2020
Expiry date:	30th March 2022
Call-Off Contract value:	£62,350 committed to cover initial 2 years. If [redacted]
Charging method:	Monthly in Arrears
Purchase order number:	TBC

This Order Form is issued under the G-Cloud 11 Framework Agreement (RM1557.11).

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

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

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

From: the Buyer	Food Standards Agency Buyer's main address: Clive House 70 Petty France Westminster London SW1H 9EX

To: the Supplier	Aetopia Limited Supplier's address: 186 Lisburn Road Belfast Northern Ireland BT9 6AL
Together: the 'Parties'	

Principle contact details

For the Buyer:	[redacted]
For the Supplier:	[redacted]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 31st March 2020 and is valid until 30th March 2022
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for 2 periods of 12 months each, by giving the Supplier 2 weeks written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud software

G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: • Setup and migration • Training • Hosting and Storage • Implementation
Additional Services:	N/A
Location:	The Services will be delivered across the FSA sites
Quality standards:	All documentation and deliverables must be delivered to the Buyer in an acceptable standard. This will be in-line with good industry practices and the Buyer will have final approval.
Technical standards:	The technical standards required for this Call-Off Contract should be in-line with good industry standards and practices
Service level agreement:	• The service level and availability criteria required for this Call-Off Contract are: Service Level Agreement Targets. Priority 1 – 200 points for failing • Resolve within 4 hours Core time. • Resolve within 6 hours Non-Core time. • No more than 1 failure a month. Priority 2 – 100 points for failing • Resolve within 8 hours Core time. • No more than 1 failure a month. Priority 3 – 50 points for failing • Resolve within 17 hours Core time. • No more than 4 failures per month. Breach of Contract triggered if points exceed: • 250 in 1 month. • 450 in a calendar quarter. • 700 bi-annually (Apr-Sep/Oct-Mar).
Onboarding:	The onboarding plan for this Call-Off Contract is: The supplier will complete the onboarding process by delivering an alpha, beta and live solution, including training for FSA staff as document in Schedule 1.
Offboarding:	The offboarding plan for this Call-Off Contract is to be agreed at the outset of the Call-Off Contract by the FSA and Aetopia
Collaboration agreement:	Not Applicable
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed 125% of the charges by the Buyer to the supplier during the call off term. The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off

	Contract Term. The annual total liability for all other defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance:	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● [professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)] ● [employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law]
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit:	Not Applicable
Buyer's responsibilities:	Not Applicable
Buyer's equipment:	Not Applicable

Supplier's information

Subcontractors or partners:	Not Applicable

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method:	The payment method for this Call-Off Contract is BACS.
Payment profile:	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details:	The Supplier will issue electronic invoices. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to [redacted]
Invoice information required – for example purchase order, project reference:	All invoices must include a valid PO number and FS430486
Invoice frequency:	Invoice will be sent to the Buyer.
Call-Off Contract value:	The total value of this Call-Off Contract is £62,350, as per breakdown in Schedule 2, over the initial 2 year Call-Off Contract length. [redacted]

Call-Off Contract charges:	The breakdown of the Charges – See Schedule 2

Additional Buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones: See Schedule 1
Guarantee:	Not Applicable
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:	N/A
Public Services Network (PSN):	N/A
Personal Data and Data Subjects:	Confirm whether either Annex 1 or Annex 2 of Schedule 7 is being used: Annex 1

1. Formation of contract

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

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

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

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.

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

Signed:	Supplier	Buyer

Name:	[redacted]	
Title:		
Signature:		
Date:	27 March 2020	30 March 2020

Schedule 1 - Services

FSA Requirements & Clarification Questions Document

Background

The National Food Crime Unit (NFCU) is a dedicated function within the Food Standards Agency (FSA), an independent non-ministerial department working across England, Wales and Northern Ireland to protect public health and consumers' wider interests in relation to food.

In response to the identification of horse meat in beef products across the UK in 2013, the Government commissioned an independent review, led by Professor Chris Elliott, to identify and propose solutions to address weaknesses in the UK's food supply networks. The Elliott Review[1] made several recommendations, including the creation of a national food crime unit. In response, the Government agreed to create a food crime unit to provide a focus to enforcement efforts against fraud and criminality in food supply chains. The NFCU became operational in December 2015 to:

> ***"…give greater focus to enforcement against food fraud in government by analysing intelligence, initiating investigations and liaising with other criminal and regulatory enforcement agencies".***

A subsequent review[2] was chaired by David Kenworthy (formerly Chair of UK Anti-Doping and Chief Constable of North Yorkshire Police) and considered the UK's response to food crime, including the existing form and function of the NFCU to determine whether this met the existing and future demand. This review recommended that the NFCU have both an *intelligence* and *investigative* capability and has as part of its remit the prevention of food crime, the responsibility for setting standards for investigating food crime and responsibility for training staff from partner agencies in food crime awareness and intelligence handling.

In March 2019 the NFCU implemented a new Case Management System (Clue) to support their case load from initial intelligence gathering through to prosecution and beyond. The NFCU have access to services such as PNC, PND and have PSN-P connectivity

[1] The Elliott Review of the Integrity and Assurance of Food Supply Networks, 2014

[2] The Kenworthy review was completed in 2016 to review the operation of the current NFCU and propose options for future improvements

Introduction

The FSA requires a DAMS to support the investigation into Food Crime to ensure any digital data is securely and correctly handled, stored and audited from initial intelligence gathering through to prosecution. Any new system would need be commercially agreed and signed by 31st March 2020 and to have an Alpha start by 6h April 2020 to a subset of users, A Beta release by 18th May 2020 and with full delivery thereafter.

The solution will allow NFCU officers to work collaboratively, upload, store, analyse, manage and share digital assets securely from their food crime caseload from initial intelligence gathering through to prosecution and beyond.

The solution is being considered for the NFCU only now but could potentially be rolled out to other teams within the FSA. Any solution must be capable of exceptional growth in volume, so it does not affect the performance of the system.

Scope

In order for a successful transition to a new DAMS there will be a 3 phase roll out. An Alpha will be rolled out to a subset of users for testing and manual data migration from the NFCUs temporary storage (not in scope for supplier). This will enable NFCU officers to smoothly transition to a new system that has been tested by users from all departments to ensure it meets their needs and to discharge their duties to purse food crime. A Beta roll out to all users to ensure business process are in place and further testing on the solution.

The following proposed distinction between Alpha functionality (April 2020), Beta functionality (May 2020) and full roll out (thereafter) is provided:

Contract Award **(31st March 2020)**	Contract awarded and signed All commercials agreed by FSA and supplier.
In scope for Alpha **(6th April 2020)**	Access to DAMS via a web browser from a desktop or laptop device) Uploading digital assets from a desktop. Viewing digital assets from a desktop. Ability to edit digital assets from a desktop Ability to search for digital assets from a desktop Sharing digital assets from a desktop Retention rules, policy and dates in places for any assets uploaded Full audit for any assets accessed, edited or deleted
In Scope for Beta **(18th May 2020)**	Access to DAMS for all users via a web browser from a desktop or laptop device) Uploading digital assets from a desktop. Viewing digital assets from a desktop. Ability to edit digital assets from a desktop Ability to search for digital assets from a desktop Sharing digital assets from a desktop Retention rules, policy and dates in places for any assets uploaded Full audit for any assets accessed, edited or deleted Ability to upload digital assets via a mobile device All users trained
In Scope for full roll out **(26th June 2020)**	All users able to Access DAMS via a web browser from a desktop or laptop device) Issue resolution Final Configuration Changes

Future requirements	☐	The solution is being considered for the NFCU only now but could potentially be rolled out to other teams within the FSA. Any solution must be capable of exceptional growth in volume, so it does not affect the performance of the system.

[redacted]

Given the NFCU's preference for direct training, Aetopia proposes a training package as follows:

[redacted]

[redacted]

Integration	5	Please clarify how your solution can link with data that is stored outside of the CMS (e.g. Case management solution (Clue) EDRMS or other solution for managing high volume data – i.e. documents, images, video, etc.)	**250**

Response:

[redacted]

Network	6	How does the solution manage the degradation to the FSAs network and other solution uses when uploading large digital assess i.e. video	**250**

Response:

[redacted]

Digital Asset Management Functional Requirements

Ref	Category	Requirement	Priority	Notes	Supplier Response -	Supplier Response - If No, please
DAMS01	Uploading	The solution must be capable of uploading digital assets individually or in bulk.	1		Yes	
DAMS02	Uploading	The solution must scan/check all new digital assets to ensure they are free from viruses.	1		Yes	
DAMS03	Uploading	The solution should allow user outside of the NFCU (FSA, Public, LAs, Police, Forensic, private	2	Public collection functionality or portal	Yes	
DAMS04	Uploading	The solution must allow users outside of the NFCU to upload digital assets only if they have been	1		Yes	
DAMS05	Uploading	The solution must allow users to upload a variety of file types to the system.	1	Please provide details of file types not supported	Yes	
DAMS06	Uploading	The solution must have the ability to blacklist some filetypes	1		Yes	
DAMS07	Uploading	The solution must automatically assign a URN to each digital asset	1		Yes	
DAMS08	Uploading	The solution should allow users to add multiple, configurable tags to digital assets	2		Yes	
DAMS09	Uploading	The solution should allow users to write notes against digital assets	2		Yes	
DAMS10	Uploading	The solution must allow users to upload digital assets from a variety of devices and end points.	1	Mobiles, Tablets, laptops, memory cards etc. Endpoints e.g. a	Yes	Yes for these examples, except for
DAMS11	Uploading	The solution could allow a system admin to limit file sizes that can be uploaded to the system	3		Yes	
DAMS12	Metadata	The solution must allow metadata to be uploaded and linked to the digital assets	1		Yes	
DAMS13	Metadata	The solution must retain any metadata that is already associated to the digital assets	1		Yes	
DAMS14	Metadata	The solution must automatically add metadata such as upload date and user details	1		Yes	
DAMS15	Metadata	The solution should automatically add metadata such as device name and location if available	3		Yes	
DAMS16	Metadata	The solution must display any metadata stored with an assets to a user	1		Yes	
DAMS17	Metadata	The system must allow a system admin to edit metadata manually	1		Yes	
DAMS18	Metadata	The solution should allow a system admin to make metadata fields mandatory	3		Yes	
DAMS19	Metadata	The soloution must keep any metadata incat if an assest os coppied	1		Yes	
DAMS20	Permissions	The solution must allow digital assets to have permissions around them to the level of individual	1		Yes	
DAMS20	Permissions	The solution must allow digital assets to not be downloaded from the system unless the user has the	1		Yes	
DAMS21	Permissions	The solution must allow different access permissions to be set for users e.g.: including but not limited	1		Yes	
DAMS22	Permissions	The solution must require users to go through a confirmation step before they delete any digital	1		Yes	
DAMS23	System Admin	The Solution must allow a Solution Administrator to set and update permissions for all users	1		Yes	
DAMS24	System Admin	The solution must allow a Solution administrator to set and update some system configuration	1		Yes	
DAMS25	System Admin	The solution must allow a system administrator the ability to add users, remove users and reset	1		Yes	
DAMS26	System Admin	The solution must allow the system admin to have access to the whole system by default	2		Yes	
DAMS27	View	The solution must have the ability to playback/preview digital assets including but not limited to,	1		Yes	
DAMS28	View	The solution must have the ability to view PDFs and documents	1		Yes	
DAMS29	View	The solution must be capable of storing and displaying multiplex CCTV footage.	1		Yes	
DAMS30	Edit	The system must have the ability to edit files, including but not limited to Clipping, image capture,	1		Yes	
DAMS31	Edit	The system should have the ability to edit image digital assets including but not limited to:	2		Yes	
DAMS32	Edit	The solution must preserve the original file without modification When editing a Digital Asset	1		Yes	
DAMS33	Edit	The solution should have the ability to redact or picticlation from vidios or pictures	1		Yes	
DAMS34	Edit	The soloution should have the ability to merge folders together.	3		Yes	
DAMS35	Searching	The solution must allow users to search for assets they have permission to view	1		Yes	
DAMS36	Searching	The solution must have a comprehensive built in search on the full range of assets and metadata	1		Yes	
DAMS37	Audit	The solution should only allow a user to see the audit trail if they have the permissions to view the	1		Yes	
DAMS38	Audit	The solution must record user searches in the Audit trail	1		Yes	
DAMS39	Audit	The solution must record in the audit when an assets has been shared with a third party	1		Yes	
DAMS40	Audit	The Solution must provide a reportable, exportable, full audit trail, identifying device (if possible),	1		Yes	
DAMS41	Sharing	The solution must allow users to share digital assets securely with third parties.	2		Yes	
DAMS42	Sharing	The solution must record an audit trail of any assets that have been shared	1		Yes	
DAMS43	Sharing	The solution could set an expiry date of how long a third party can share digital assets	3		Yes	
DAMS44	Sharing	The solution could allow different access permission when sharing assets with third parties e.g. view	3		Yes	
DAMS45	Retention	The solution must allow retention dates to be set on all digital assets.	1		Yes	
DAMS46	Retention	The solution must flag when an assets is nearing the retention date.	1	Configurable time	Yes	
DAMS47	Retention	The solution must meet DPA and be fully compliant to meet DPA	1		Yes	
DAMS49	Retention	The Solution should have the capability to delete records and inbuilt review workflow based on	3		Yes	
DAMS50	Retention	The Solution must have a process in place to flag up regular retention period reviews of data and	2		Yes	
DAMS51	Retention	The solution should allow the purging / weeding of data automatically according to the age of the	2		Yes	
DAMS52	Retention	The soultion should meet ISO 17025	2		Yes	
DAMS53	Reporting,	The solution should be able to provide FSA with management reporting and usage of the solution e.g.	2		Yes	
DAMS54	Reporting,	The solution should have a dashboard function to show high level management reporting	2		Yes	
DAMS55	Reporting,	The solution should have an alerting and notification function e.g. when assets have been added or an	2		Yes	
DAMS56	Integration	The system should be able to work in conjunction with the NFCUs CMS system other FSA system.	2	The NFCUs CMS system is Clue	Yes	
DAMS57	Integration	The solution should be able integrate with other NFCU and FSA systems.	2		Yes	
DAMS58	Storage	The NFCU have identified there will have 3 type of digital assets:	1	How does your solution store these types of assets?	Yes	Media assets are stored on a secure
DAMS59	Future	The solution must be capable of expediential growth in the volume and type of Digital Assets, so it	1		Yes	
DAMS60	Future	The Supplier must provide the ability to develop the application, in tandem with NFCU based on	1		Yes	
DAMS61	Future	The Solution should as far as possible be designed to upload Digital Assets from future data sources, e.g. smart/digital houses, smart/digital/self-driving cars, smart/digital cities etc.	1		Yes	
End of Clarification Questions						

Digital Asset Management System Non-Functional Requirements

Ref	Category	Requirement	Priority	Notes	Supplier Response - Meet Requirement Y/N ONLY	Supplier Response - If No, please briefly state why (no more than 50 words)
NFR001	Business Standards	The Supplier should hold professional recognised accreditations that would be pertinent for this contract.	2		Yes	
NFR002	Managed Service	The Supplier must provide a comprehensive ITIL compliant support function based on process models from	1		Yes	
NFR003	Managed Service	The Supplier should declare where Services or Components are being provided by third parties or	2		Yes	
NFR004	Managed Service	The Supplier must, alongside the Agency, change and adapt the service portfolio when required, to reflect	1		Yes	
NFR005	Managed Service	The Supplier must adhere to the NFCU standard set of SLAs and service point structure (provided)	1	Copy of standard SLAs and service	Yes	
NFR006	Licensing	All licence statements and associated terms of use must be provided to the Agency by the Supplier on an	1		Yes	
NFR007	Licensing	The Supplier must indicate whether the Agency, the Supplier, Trusted Partner or Third Party are providing	1		Yes	
NFR008	Training	The Supplier must provide end user training. This may include but not be limited to:	1	Detail required for implementation	Yes	
NFR009	Project Management	The Supplier must provide a high level implementation plan demonstrating key stages for the project,	1	Detail required for implementation	Yes	
NFR010	Project Management	The supplier must be able to implement an Alpha by 15th May 2020	1		Yes	
NFR011	Project Management	The Supplier must identify the resources required for implementation and configuration and for that	1		Yes	
NFR012	Project Management	The Supplier must maintain and provide standard project documentation to satisfy the Agency project	1	Detail required for implementation	Yes	
NFR013	Project Management	The Supplier must ensure the correct and adequate resource is allocated to the project from the outset	1	Detail required for implementation	Yes	
NFR014	Project Management	The Supplier must not change the key personnel unless by prior agreement with the Agency or at the request	2		Yes	
NFR015	Accessibility and Usability	The Solution should be intuitive, easy to use and have the ability for personal and/or global configuration.	2		Yes	
NFR016	Accessibility and Usability	The Solution should meet the latest UK Government accessibility recommendations when presented via a	2		Yes	
NFR017	Accessibility and Usability	The Solution must be compatible with the latest version of the most common browsers, specifically Chrome.	1		Yes	
NFR018	Accessibility and Usability	The Solution should give the user access to a help function that gives usage advice for each of its features	2		Yes	
NFR019	Availability and Continuity	The Supplier must provide high availability and business continuity to the Agency. The current operating	1		Yes	
NFR020	Availability and Continuity	The Supplier must provide comprehensive and effective Disaster recovery services. This may include but not	1	Detail required for implementation	Yes	
NFR021	Performance and Monitoring	The Supplier must provide adequate capacity, monitoring, reporting and work with the Agency to investigate	1		Yes	
NFR022	Performance and Monitoring	The Solution should provide mechanisms to automatically notify the Agency if the Solution or components of	2		Yes	
NFR023	Performance and Monitoring	The Solution must deliver an acceptable round-trip latency for the User from request to response. (under 5	1		Yes	
NFR024	Performance and Monitoring	The Supplier should flex capacity (up or down) where necessary, without a negative impact on the Service.	2		Yes	
NFR025	Performance and Monitoring	The Supplier should confirm that there will be no detrimental impact on the Agency' local or wide area	2		Yes	
NFR026	Hosting	The Solution must be hosted and supported in the UK as a full SAAS offering	1		Yes	
NFR027	Hosting	The Supplier must provide a High Level Design for the Solution covering all environments. This may include	1	Detail required for implementation	Yes	
NFR028	Hosting	The Supplier must provide multiple environments to facilitate testing, training and development.	1		Yes	
NFR030	Hosting	Accommodation of hardware and systems owned by or procured for and on behalf of the Agency must be	1		Yes	
NFR031	Hosting	Data Centres utilised for the provision of hardware and systems representing the Agency Solutions must	1		Yes	
NFR032	Hosting	The accommodation should be certified to ISO 14001 (environmental management) and should note whether	2		Yes	
NFR033	Hosting	The accommodation should be certified to ISO 50001 (energy management).	2		Yes	
NFR034	Hosting	The Hosting provider should be certified to ISO 27001 (Information Security Management).	2		Yes	
NFR035	Hosting	The Supplier should allow and detail their processes for giving access to the Agency if they wished to visit the Data Centre location.	2		Yes	This would be subject to approval by Amazon Web Services UK
NFR036	Hosting	The Supplier will ensure that any FSA Data which it causes to be transmitted over any public network (includin	1		Yes	
NFR036	Identity, Authentication and	The Solution should integrate with the Authorities' Microsoft Active Directory to authenticate access (SSO)	2		Yes	
NFR037	Identity, Authentication and	The Solution should be able to define the roles and permissions the Authorities' users and administrators	1		Yes	
NFR038	Identity, Authentication and	The supplier must provide an access control regime that ensures all users and administrators of the Supplier S	1		Yes	
NFR039	Identity, Authentication and	The Supplier must apply the 'principle of least privilege' when setting access to the Supplier System/Service s	1		Yes	
NFR040	Identity, Authentication and	Retain records of access to the Supplier System/System and make then available to the FSA on request for sup	2		Yes	
NFR041	Identity, Authentication and	The Supplier should automatically log a user out after a configurable period of user inactivity.	1		Yes	
NFR042	Identity, Authentication and	The Supplier must provide configurable role based access, administered by NFCU	1		Yes	
NFR043	Identity, Authentication and	The Solution must not allow multiple logins from the same account at the same time	1		Yes	
NFR038	EUD	The Solution must work on the agency EUD build (Windows 10, Office 365, Chrome) and if appropriate retain	1		Yes	
NFR039	EUD	The Solution should allow Users the ability to consume the Service regardless of the End User Device i.e.	2		Yes	
NFR040	EUD	The Supplier will ensure that any FSA Data which resides on a mobile, removable or physically uncontrolled de	1		Yes	
NFR041	EUD	The Supplier will ensure that any device which is used to Process FSA Data meets all of the security requireme	1		Yes	
NFR040	Technical Standards	The Solution should align to the FSA's TDA principles.	2	Copy of TDA principles included in	Yes	
NFR041	Testing	The Supplier must provide comprehensive end to end testing. This may include but not limited to	1	Detail required for implementation	Yes	
NFR042	Testing	The Supplier must provide effective detection, defect error reporting and resolution	1		Yes	
NFR043	Testing	The Supplier should provide a full test plan for full implementation including all resource requirements	2	Detail required for implementation	Yes	
NFR044	Testing	The Supplier should include sign off milestones for the Agency within the test plan.	2		Yes	
NFR045	Testing	The supplier must ensure defect fixing is in line with the project and solution development approach (e.g.	1		Yes	
NFR046	Testing	The Agency reserve the right to attend and witness all inspections and testing, both during the initial	2		Yes	
NFR047	Testing	The Supplier must act as a single point of contact for all testing activities irrespective of whether the	1		Yes	
NFR048	Testing	The Supplier must provide the Agency with the capability to fully test new releases, outside of the live	1		Yes	
NFR049	Testing	The Supplier must carry out independent annual penetration/security testing on their infrastructure and	1		Yes	
NFR050	Testing	The Supplier must detail their patching test strategy detailing how patches are tested before being applied	1		Yes	
NFR051	Testing	The Supplier must be able to provide a copy of the report of an IT Health Check conducted in the last 12 montl	1		Yes	
NFR052	Data Protection Compliance	The Supplier must ensure and confirm that the data being hosted and represented for the FSA is physically	1		Yes	
NFR053	Data Protection Compliance	The Solution must be compliant with the Data Protection Act 2018 (specifically Schedule 3 for FSA)	1		Yes	
NFR054	Data Protection Compliance	The Suppliers system and processes must ensure:	1		Yes	
NFR055	Data Protection Compliance	The solution must effectively support the FSA to manage, notify and respond to individual GDPR rights	1		Yes	
NFR056	Data Protection Compliance	The Supplier must have systems to meet GDPR records of processing requirements and processes to	1		Yes	
NFR057	Data Protection Compliance	The Supplier must have systems, processes and measures to ensure processors/ sub-processors meet data	1		Yes	
NFR058	Data Protection Compliance	The supplier must have staff trained in data protection requirements, policies and processes	1		Yes	
NFR059	Policies and Assurance	The Supplier will provide copies of their data protection policy to the FSA	2		Yes	
NFR060	Data & Information Governance	The Supplier must ensure that data entered is consistent at the point of entry where appropriate to ensure	1		Yes	
NFR061	Data & Information Governance	The Solution must ensure that date and time data held in the system is Coordinated Universal Time (UTC)	1		Yes	
NFR062	Retention Deletion and	The Supplier must ensure the FSA can apply data archiving and retention policies to the System/Service	1		Yes	
NFR063	Retention Deletion and	The Solution must allow FSA./Supplier to rectify, erase or update incomplete data and delete information in	1		Yes	
NFR064	Retention Deletion and	The supplier should have documented processes to ensure the availability of FSA Data in the event of the Sup	2		Yes	
NFR065	Retention Deletion and	securely erase in a manner agreed with the FSA any or all FSA Data held by the Supplier when requested to do	1		Yes	
NFR066	Retention Deletion and	securely destroy in a manner agreed with the FSA all media that has held FSA Data at the end of life of that me	2		Yes	
NFR067	Retention Deletion and	The supplier must have processes which address the CPNI and NCSC guidance on secure sanitisation	1		Yes	

NFR068	Data Import/Export	The solution must allow for scheduled (automated) or manual export of data from other systems or sources	1		Yes	
NFR069	Data Import/Export	The solution must allow for scheduled (automated) or manual import of data from other systems or sources	1		Yes	
NFR070	Data Import/Export	The solution must have the ability to bulk migrate data from a legacy system into the System/Service and	1		Yes	
NFR071	Data Standards	The supplier must work with the FSA data architects to ensure any relevant data standards are adhered to	1		Yes	
NFR072	Security	The Supplier must agree to follow the principles of security confidentiality, integrity and availability of the	1		Yes	
NFR074	Security	The Supplier will provide copies of their security patching, monitoring access and security policies to the FSA	1		Yes	
NFR075	Security	The Supplier will notify the FSA immediately if they identify a new risk to the components or architecture of	1		Yes	
NFR076	Security	The Supplier will regularly review the agreed security documentation and policies	2		Yes	
NFR077	Security	If the Supplier becomes aware of a Breach of Security including a Personal data breach the Supplier will inforn	1		Yes	
NFR078	Security	The Supplier as a minimum must to do the following upon it becoming aware of a Breach of Security or	1		Yes	
NFR080	Security	The Supplier must ensure all staff who have physical or logical access to NFCU data or admin rights to domain	1		Yes	
NFR081	Security	The Supplier shall not permit Supplier Personnel who fail the security checks rto be involved in the managem	1		Yes	
NFR082	Security	The Supplier shall collect audit records which relate to security events that would support the analysis of pote	1		Yes	
NFR083	Security	The Supplier and the FSA shall work together to establish any additional audit and monitoring requirements	2		Yes	
NFR084	Security	The retention periods for audit records and event logs must be agreed with the FSA and documented	2		Yes	
NFR085	Security	The Supplier shall not and shall ensure that none of its Sub-contractors Process FSA Data outside the EEA (incl	1		Yes	
NFR086	Security	The severity of vulnerabilities shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' these	1		Yes	
NFR087	Vulnerabilities and Patching	The Supplier shall apply security patches to vulnerabilities in the System/Service within: 7 days after the publ	1		Yes	
NFR088	Security	The Supplier must give a brief overview and supply a design of the systems and architecture that will be used	1		Yes	
NFR089	Security	The Supplier must ensure the system service is designed in accordance with the NCSC "Security Design Princip	1	https://www.ncsc.gov.uk/guidance/s	Yes	
NFR090	Security	The Supplier must ensure the System./Service is designed in accordance with the NCSC "Bulk Data Principles"	1	https://www.ncsc.gov.uk/guidance/pr	Yes	
NFR091	Security	The supplier must ensure the System/Service is designed in accordance with the NSCS "Cloud Security Princip	1	https://www.ncsc.gov.uk/guidance/l	Yes	
NFR092	Maintenance	The Supplier must undertake all non urgent upgrades to the live system outside of "core hours" which are	1		Yes	
NFR093	Maintenance	The Supplier must provide a roadmap for their software and the anticipated release dates for upgrades.	1		Yes	
NFR094	Maintenance	Upgrades must be provided as part of the overall baseline costs and will not be charged on a 'per upgrade'	1		Yes	
NFR095	Maintenance	The Supplier should provide details of any user groups that provide feedback to the Supplier on suggested	2		Yes	
NFR096	Maintenance	The Solution must allow for local configuration changes to take place. This may include but not be limited to:	1		Yes	
NFR097	Scalability	The Solution must be scalable to increase or decrease User Capacity without Performance degradation	1		Yes	
NFR098	Scalability	The Solution must be scalable to increase or decrease Compute Capacity without Performance degradation	1		Yes	
NFR099	Scalability	The Solution must be scalable to increase or decrease Live Storage Capacity without Performance	1		Yes	
NFR100	Scalability	The Solution must be scalable to increase or decrease Archive Storage Capacity without Performance	1		Yes	
NFR101	Value	The Solution must allow NFCU data to be exported on system retirement in multiple non proprietary usable	1		Yes	
NFR102	Value	The Supplier must ensure the NFCU is on the latest released version of the application within 6 weeks of	1		Yes	
NFR103	Value	The Supplier must provide a high level exit strategy and indicative costs if the Agency decide to stop using	1	Detail required for implementation	Yes	
NFR104	Mobile Devices	The system should be operational on a wide spectrum of operating conditions, such as different screen sizes, performance and internet connection speed, trough an application or browser. If no please provide comments if it is on your roadmap	2	The FSA device default is Android minimum version 8.1 - Samsung J5, J6 and A40. There are also a number of iOS devices in the organisation minimum iOS version is 12.1. All device are fully managed by Intune	Yes	
NFR105	Mobile Devices	The system should make effective use of input devices on the mobile device. For example, the camera	2		Yes	

Additional Non-Functional Requirement:

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 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.

Aetopia Response:

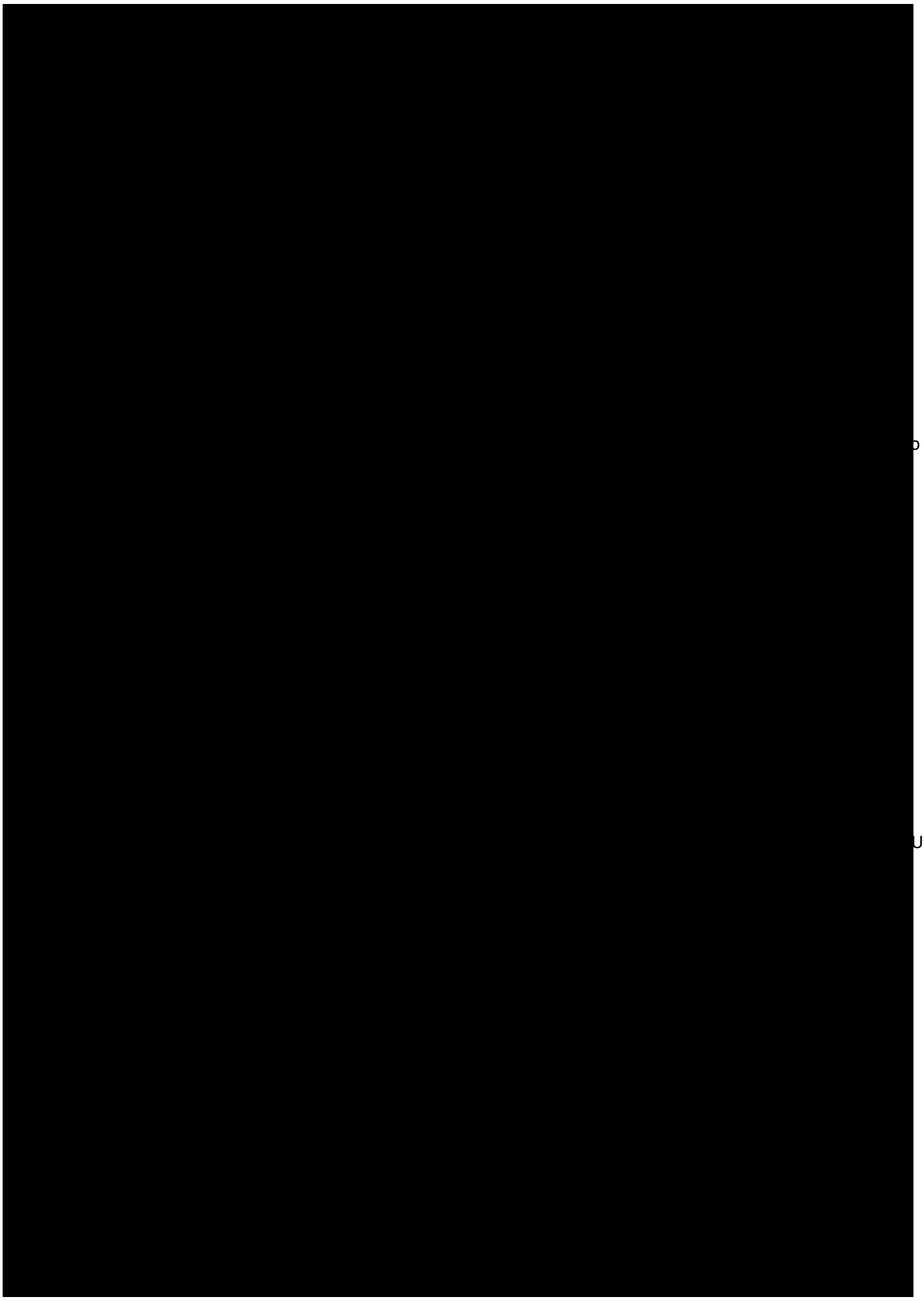
Yes, we are happy to comply with HMG pre-employment checks.

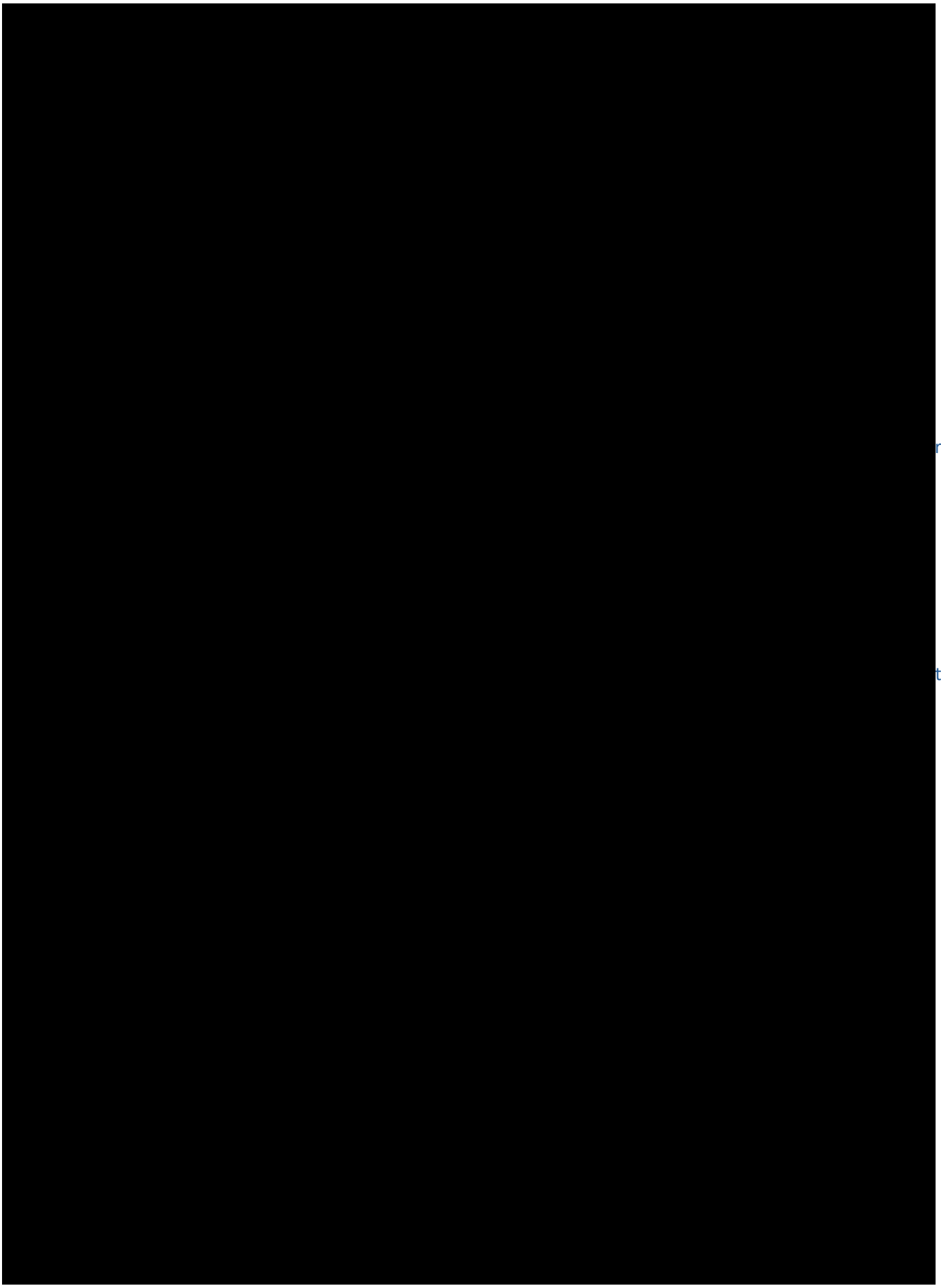
Schedule 2 - Call-Off Contract charges

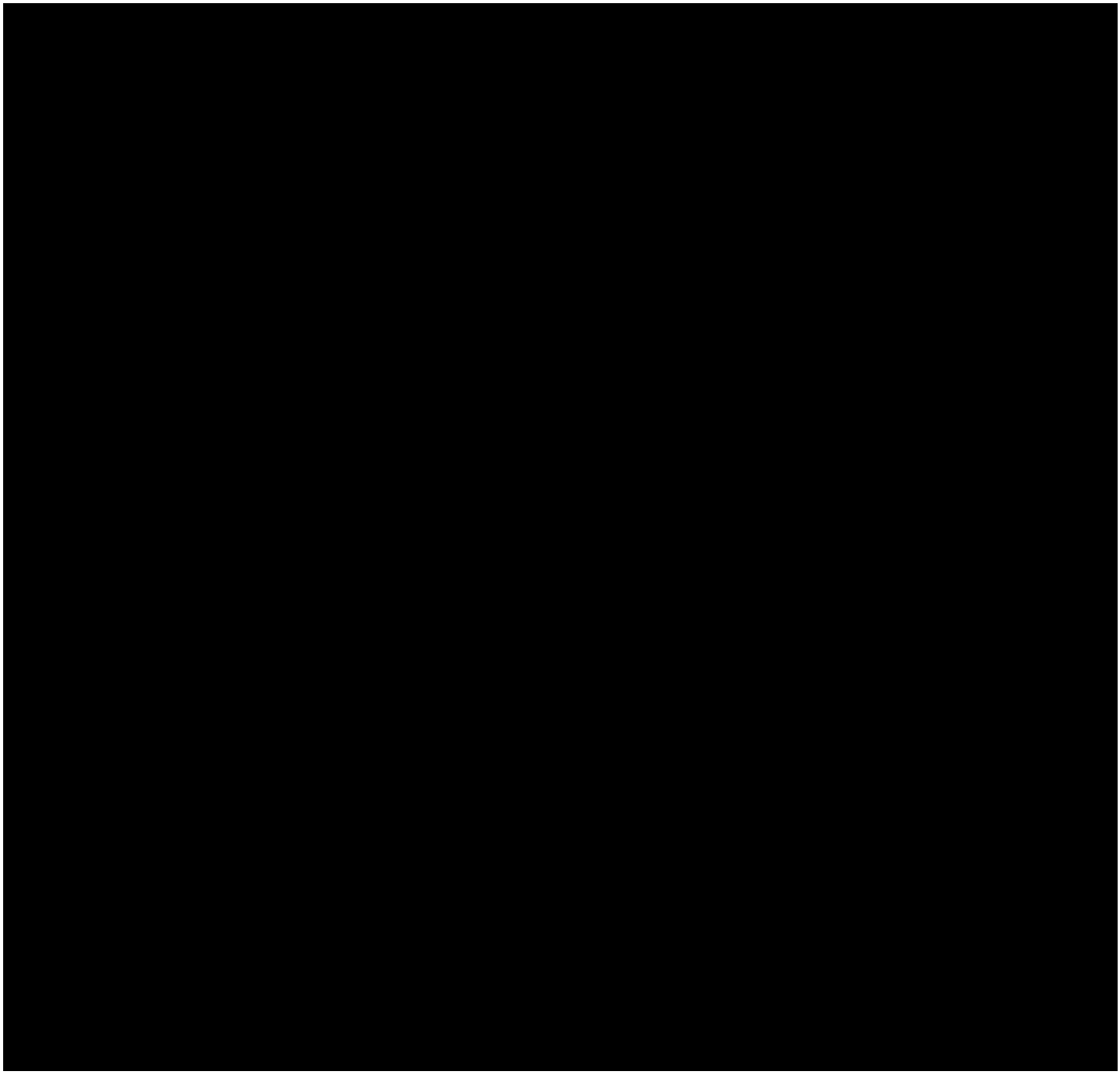
Annual subscription and storage costs

Item	Cost
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]







Part B - Terms and conditions

1. Call-Off Contract start date and length

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

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)

- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in schedule 4 (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:

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

before the date on which the tax or other liability is payable by the Buyer.

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers

liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

- a broker's verification of insurance
- receipts for the insurance premium
- evidence of payment of the latest premiums due

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

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

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

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

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

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

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.78 to 8.86. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

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

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

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

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

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

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

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

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

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

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

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

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

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

13. Buyer data

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

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

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

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

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

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

- the principles in the Security Policy Framework at

https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications

- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/collection/risk-management-collection
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

- an executed Guarantee in the form at Schedule 5
- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

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

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry

- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)

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

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

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

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

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

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

- work with the Buyer on any ongoing work

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

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

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

20. Notices

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

Manner of delivery	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error message

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

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

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

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

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

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

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

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

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- other information reasonably requested by the Buyer

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

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

23. Force majeure

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

24. Liability

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

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

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

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

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

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

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

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

- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will

indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

- work proactively and in good faith with each of the Buyer's contractors
- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

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

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their

G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this 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, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7

Schedule 3 - Collaboration agreement

Not Applicable

Schedule 4 - Alternative clauses

Not Applicable

Schedule 5 - Guarantee

Not Applicable

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 Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited

	to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.

End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.11 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.

G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company

	● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.

Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's 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 Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-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.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1 - Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are: informationmanagement@food.gov.uk
1.2 The contact details of the Supplier's Data Protection Officer are: dataprotection@aetopia.co.uk
1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ***The subject matter of the Processing is the Buyer – namely the National Food Crime Unit***
Duration of the Processing	*The duration of the Processing shall be from the start date of this Call-Off Contract until the expiry or early termination of this Call-Off Contract*
Nature and purposes of the Processing	*Purposes of the Processing is to facilitate the use of the Digital Asset Management System* *The nature of the Processing shall include: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means)* *The Buyer Personal Data is being processed by the Supplier to*

	enable the Supplier to provide the Services set out in this Call-Off Contract to the Buyer.
Type of Personal Data	*The types of Buyer Personal Data that will be processed by the Supplier include any type of personal data including but not limited to the following that is required to be captured as part of the Digital Asset Management System processes: First Name, Surname, Date of Birth, Place of Birth (Town/Region/Country), Nationality, Address, Email Address, Contact Telephone Number, Unique Identification Numbers, Various supporting documentation, and any other appropriate data recorded as part of end-to-end processes supported by the NFCU.*
Categories of Data Subject	*FSA Staff (including volunteers, agents, and temporary workers), personal data originating from the NFCU's food crime caseload.*
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	*Upon expiry of the contract the Processor will return all data to the Buyer.*

Annex 2 - Joint Controller Agreement

Not Applicable