Crown Commercial Service

G-Cloud 10 Call-Off Contract

This Call-Off Contract for the G-Cloud 10 Framework Agreement (RM1557.10) includes:

Part A - Order Form

Digital Marketplace service ID number:	3894 1431 6063 429
Call-Off Contract reference:	CQC EAF 028
Call-Off Contract title:	Personal Safety Monitoring System
Call-Off Contract description:	Personal safety monitoring service, to be hosted by a third party who would monitor Inspectors visiting high risk premises or people or working out of hours. The main features of such a service include: An SOS safety device with one button alarm activation. This may be a stand-alone device or via an app on existing mobile phones. 24/7 support via an Incident Management Centre GPS tracking Two way audio with qualified security staff Clear emergency escalation process Welfare check management Safe Hub for Android Smartphone
Start date:	25/02/2019
Expiry date:	24/02/2024
Call-Off Contract value:	£150,000 Excluding VAT £180,000 Including VAT based on a minimum of [redacted] Staff volumes have the potential to increase and decrease over the term.
Charging method:	Invoice
Purchase order number:	TBC

This Order Form is issued under the G-Cloud 10 Framework Agreement (RM1557.10).

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	Care Quality Commission Buyer's phone: 0207448 9086 Buyer's main address: 151 Buckingham Palace Road 3rd Floor London SW1W 9SZ
To: the Supplier	Mitie Limited 0330 678 0710 Supplier's address: The Shard Level 12 32 London Bridge Street London SE19SG Company number: 2938041
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: [redacted] Name: [redacted] Email: [redacted] Phone: [redacted]
For the Supplier:	Title: [redacted] Name: [redacted] Email: [redacted] Phone: [redacted]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 25/02/2019 and is valid for 60 months.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least (60) Working Days from the date of written notice for disputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period:	N/A

Buyer contractual details

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

G-Cloud Lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud software
G-Cloud services required:	Smartphone based Safe Hub lone worker app (smartphones supplied by CQC). The service will consist of: • Access to the Lone Worker Manager Portal/Platform • 24/7 ARC response • Ongoing online access to training materials • Multi-network SIM • Mobile application with additional Safe Check and Group Alert risk messaging features • Fully managed service including 7 day per week Support Desk • Customised reporting dashboard and web-portal • Proactive account management team
Additional services:	1st line technical support will be provided by the Mitec ARC 24/7 2nd line technical support will be available 7 days per week between 09:00 and 17:30
Location:	The Services will be delivered to the following address: N/A
Quality standards:	The quality standards required for this Call-Off Contract are BS5979, BS8484 and ISO27001.
Technical standards:	The technical standards required for this Call-Off Contract are BS5979, BS8484 and ISO27001.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are 1. Verification of 80% of all alerts by an ARC Operator in 10 seconds 2. Verification of 98.5% of all alerts by an ARC Operator in 40 seconds 3. 100% of Support Queries responded to within 4 working hours
Onboarding:	The onboarding plan for this Call-Off Contract is [enter text]. Example Mobilisation Plan
Offboarding:	The offboarding plan for this Call-Off Contract: Mitie will supply CQC with a CSV of all of its employee data. This can be used to pass to an alterbative supplier, should CQC wish to do so.

Collaboration agreement:	N/A
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed £1,000,000. 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 (whichever is the greater). The annual total liability for all other defaults will not exceed the 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
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 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 limit of £5,000,000 or any higher 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 7 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. Both parties agree to work together regarding audit requirements.
Buyer's responsibilities:	The Buyer is responsible for The Buyer is responsible for providing accurate and timely information as required, arrangement of regular supplier meetings, consultation on the design and provision of new products and services, and escalation of concerns in a timely manner.
Buyer's equipment:	The Buyer's equipment to be used with this Call-Off Contract includes smart phones. It is anticipated that the Supplier will provide their own Computer equipment in order to conduct the services unless they request otherwise.

Supplier's information

Subcontractors or partners:	[redacted]

Call-Off Contract charges and payment

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

Payment method:	The payment method for this Call-Off Contract is BACS.
Payment profile:	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details:	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to:. Care Quality Commission T70 Payables F175 Phoenix House Topcliffe Lane Wakefield West Yorkshire WF3 1WE
Invoice information required – for example purchase order, project reference:	All invoices must include Purchase Order number TBC
Invoice frequency:	Invoice will be sent to the Buyer TBC.
Call-Off Contract value:	The total value of this Call-Off Contract is up to £467,280 Including VAT based on 1947 staff.
Call-Off Contract charges:	The breakdown of the Charges is: Contract duration 60 months Cost of app per person per month [redacted] Annual cost based on [redacted] Total Contract £180,000

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: • TBA at Mobilisation Planning Meeting
	Mitie has excellent financial standing. Credit check welcome
Warranties, representations:	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that [enter any additional warranties and representations]. [Delete if not relevant.]
Public Services Network (PSN):	The Public Services Network (PSN) is the Government's secure network. If the G-Cloud Services are to be delivered over PSN this should be detailed here: [enter text]. [Delete if not relevant.]
Personal Data and Data Subjects:	Will Schedule 7 – Processing, Personal Data and Data Subjects be used Yes [Delete as appropriate]

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 RM1557.10.

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

Signed:	Supplier	Buyer
Name:	[redacted]	[redacted]
Title:		
Signature:		
Date:		

Schedule 1 - Services

Executive Summary

The Care Quality Commission ("CQC") is a non-departmental public body established under the Health and Social Care Act 2008 and is the independent regulator of health and adult social care in England. Its purpose is to ensure that health and social care services provide people with safe, effective, compassionate, high-quality care and to encourage care services to improve.

CQC has circa 2,000 fieldwork staff who carry out the registration of health and adult social care providers, monitor inspect and rate services and carry out enforcement where poor care is identified. Some of this work is carried out outside of normal office hours and can be in remote locations or domestic settings.

Health and safety legislation places an absolute duty on CQC to ensure the health safety and welfare of staff whilst at work, this includes personal safety arrangements. To support the Lone Working & Personal Safety Code of Practice and personal safety training for

staff, CQC is seeking a supplier to provide a Personal Safety Monitoring Service to monitor staff who are either working alone and/or out of hours, or in remote or domestic settings to ensure they stay safe at the location and return safely from their appointment.

Personal Safety Monitoring Service

CQC wish to procure a formal personal safety monitoring service, to be hosted by a third party who would monitor Inspectors visiting high risk premises or people or working out of hours. The main features of such a service include:

An SOS safety device with one button alarm activation. This may be a stand-alone device or via an app on existing mobile phones.

24/7 support via an Incident Management Centre

GPS tracking

Two way audio with qualified security staff

Clear emergency escalation process

Welfare check management

The Requirement

The service should also be able to provide real time protection to staff through a range of digital solutions such as mobile phones, devices and laptop PC's.

The service must be available 24 hours a day, seven days a week, 365 days a year.

The service must also provide on line induction user training for staff.

It is an expectation that statistical management reports on trends and common factors will be available.

Data Transfer

The system must be able to accept data from CQC's Electronic Staff Record (ESR) to ensure personnel information is up to date and to avoid duplication of work. ESR is the system that holds CQC's personal HR records (updated when an employee leaves or joins CQC and throughout the entire employee lifecycle). The system will be updated on a monthly basis by means of a 'data dump' from CQC's electronic staff record (ESR) with staff information such as name, employee number, directorate, region and team etc to provide good MI reports, and as such the new system must be compatible for such uploads. The information will be transferred via CQC's SFTP solution with the most likely format being excel or csv.

Personal Safety Monitoring Service - High Level and Functional Business Requirements

Suppliers to provide a solution that addresses the high level and functional business requirements.
Suppliers must address the high level functional, non-functional and security requirements in their response to the method statement of the evaluation criteria

As part of the evaluation process the functional business requirements will be assessed in line with the evaluation criteria.

Functional Business Requirements	
High Level Requirement	Description – Functional Requirements
The system	• The provision of an SOS safety device with one button alarm activation. This may be a stand-alone device or via an app on existing Android or IOS mobile phones. • 24/7 live time support via a dedicated Alarm Receiving Centre certified to the appropriate British Standard • Call response time must meet the minimum requirements of British Standard (BS) 8484:2016 • The system must be able to accept data from CQC's Electronic Staff Record (ESR) to ensure personnel information is up to date and to avoid duplication of work • Clear verification process and measures in place. • GPS tracking facility • Two way audio with qualified security/monitoring staff • Clear emergency escalation process • Welfare check management when required • The system should link to the CQC's electronic staff record and automatically populate staff information and line management information. • There should be the flexibility to record incidents to non-staff members who carry out work for CQC in the same way as we do staff members. • There must be the ability to record information relating to an incident over an extended period of time to allow emerging evidence to be captured. • The system must have a central tracking system to enable outstanding actions to be monitored and reported until completion. • The system should automatically update a nominated CQC staff when an incident is reported, resolved and closed. • The system will be capable of reporting all incidents to the nominated Chief Inspector. Executive Directors (or equivalent) on a weekly basis to allow short term interventions to be initiated.
Management Information and Reporting	• There will be an expectation that the system will provide Senior Management with management information relating to incidents, by directorate, team and sub team; • The system should be capable of producing management information to highlight trends and dependencies year or year/month on month.
Manage cases- Search, Archive & Retrieve cases	• The system must provide a reliable clear audit trail of all incidents. • Archived information will remain in archive for the length of contract plus 3 years.

Non Functional Requirements

Suppliers to confirm that the tool being proposed is able to operate in line with

the generic saas non-functional requirements.

As part of the evaluation process generic saas non-functional requirements will be assessed in line with the evaluation criteria.

Non Functional Requirements – Generic Software as a Service
Availability requirements & support
System availability – Any system is required to meet service availability levels of 99.5% for 365 days per year, with system maintenance outside working hours
Required server environments – The following server environments are required Live, Test, Development, User Acceptance Testing, Pre-production and Training, if appropriate to the nature of the service.
Disaster recovery – System will be supported in the event of a disaster and any recovery plans will be tailored to CQC needs and be compliant with business continuity standards.
Recovery Time
Recovery time & point objective – The recovery mechanisms must support minimal recovery time with optimal recovery points.
Backup schedules - Back-ups are to be carried out completely according to documented data back-up requirements. Appropriate personnel are to verify the usability of backed-up data and retain verification evidence.
Performance & scalability
Storage – The system must handle an increase in storage requirements without major system changes or data migration activities.
System scalability - System shall be scalable both in terms of users and storage, with that easy to change both in terms of cost and minimal disruption.
Network performance and load – The system must minimise the load on CQC's network and provide mechanisms for reporting on and controlling that load.
System performance - Describe the typical response time that can be expected from an end user perspective when accessing the application, carrying out a typical task.
Integration
Integration – System must support authentication using CQC's existing active directory as part of its existing infrastructure managed service (Open Service) using ADFS.

Interface requirements - Where relevant to its function, the system shall be capable of interfacing with CQC internal and external data sources, such as Siebel CRM, OBIEE, Oracle 11g, MySql, PostgreSQL and SQLServer 2008 and above, making use of CQC's Mulesoft Anypoint platform for transactional integration. As stated in the Architecture Principles, a service oriented approach should be used, where practical and possible.
Use of mobile devices - System shall support the use of a range of mobile devices, meeting CESG requirements.
Monitoring
Application monitoring - The application must be monitored by the provider, with suitable alerting tools in place to notify of current or imminent service breaches and security issues.
Reporting
Availability reporting - Provide examples of daily, weekly and monthly application availability reporting.
Capacity reporting - provide examples of monthly reporting on current versus projected capacity, both in terms of storage and licenses.
Service Management reporting - provide examples of daily, weekly and monthly reporting on the overall performance on the service, including performance, requests and incidents relating to the service.
Change management and release process
Change management - Demonstrate your ability to perform changes to the application in a controlled and structured manner, including adherence to any methodologies.
Release Management - System to be subject to formal processes for release management, in association with customer with regard to testing.
Segregation of environments - Responsibilities related to program coding, application testing and approval, program transfer between environments are segregated
Usability
Language support - The application must support UK English.
Desktop support - All system configuration settings are remotely accessible to the system administrator through application screens or setup programs (i.e. no hard coded system variables exist and include system, user, roles, company and other configuration screens).
User experience – The solution must provide an intuitive user interface that enables the user to complete a task whilst minimising the need to navigate the system

Software as service - Customer Desktop devices are restricted in terms of the ability to download components from external sources. The system shall operate with the minimal need for software components to be applied to PC or desktop devices. The CQC standard desktop is Windows 10 32 bit with 3.5 Gb of RAM with Internet Explorer 11 and Microsoft Office 2016. The supplier must provide comprehensive systems administration, installation guides and processes, as appropriate to the nature of the service. A complete, typical deployment architecture must be described.
Compliance
Open service IT standards - The application must comply with the CQC Architecture Principles.
Legal compliance - Compliance with all UK legislative requirements including the General Data Protection Regulation, the Data Protection Act 2018, the Freedom of Information Act 2000, the Human Rights Act 1998 and any other relevant legislation
Government Technology Strategies – The system or service must comply with the U.K. Government Digital strategy
Data purging/archiving - There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.
Escrow
Source code availability - In the event of buyout or liquidation of the vendor the base source code of the software must be made available to CQC.
Support
Service desk & service manager - Supplier shall provide a service desk with the ability to log and resolve incidents and requests. The supplier shall provide a named contact for escalation of issues and regular interface between the supplier and the customer. The supplier shall detail the channels available and typical response times for both fault resolution and functional query support.
Accessibility
Accessibility – The system shall enable accessibility via assistive technology for those who cannot use a standard mouse and/or keyboard e.g. WA3, Dragon Speak and Windows 7 Voice Recognition software. It shall also enable access for those with additional visual or hearing needs. The supplier shall state how these needs are met by the software.

Non Functional Requirements – Information Security

7.1 Suppliers to confirm that the tool being proposed is able to operate in line with the information security non-functional requirements.

7.2 As part of the evaluation process the information security non-functional requirements will be assessed in line with the evaluation criteria.

Non Functional Requirements – Information Security (Please note should there be any significant security omission or compliance may result the suppliers offer not be taken forward)
Session security
Login – All user identifiers must be linked to roles which have explicit and granular assignments to access levels that enforce a restriction on the ability of the end user to create, read, update and delete information.
Password requirements – Passwords must be configurable and enable enforcement to have a minimum length of 8 characters with a mixture of lower and upper case characters and symbols, as required by CQC policies which may vary between devices. Password expiry must be configurable and able to be set to 90 days and passwords must not be able to be recycled.
Password requirements for administrator accounts – Passwords for administrator accounts must be configurable and enable enforcement to have a minimum length of 10 characters with a mixture of lower and upper case characters and symbols. Password expiry must be configurable and able to be set to 90 days and passwords must not be able to be recycled.
Inactivity timeout – Where the solution maintains a user session, it must be able to configured to timeout as needed for the particular use case.
Identity
Client applications – The solution will identify all client applications before allowing them to use its capabilities.
End users – The solution will identify all of its human users before allowing them to use its capabilities.
Physical access – All personnel will be required to present relevant identification before they are allowed access to secure locations such as CQC offices or data centres.
Single sign on – The solution will not require an individual user to identify themselves multiple times during a session (single sign on).
Inactivity – The solution must provide a mechanism for suspending user accounts when they have not been used for a predefined period.
Employee status – The supplier must prevent access to customer data and systems by employees who are leaving its employment and disclose their policy and procedures regarding this.
Authentication
Access to capabilities – The solution will authenticate all users before allowing them

to use its capabilities.
Access to user details – The solution will authenticate of all users before allowing them to update their user information.
Access by client applications – The solution will authenticate all client applications before allowing them to use its capabilities.
Authorisation
Own personal information – The solution will allow each user to access to all of their own personal information, where applicable.
Others personal information – The solution will only allow users access to the personal information of other users, where a business case for that exists.
Access restrictions – The solution will be capable of restricting access to specified areas or databases.
Password repository – The solution will not allow access to the user password or hash database / file.
Incorrect credentials – The solution will create increasing time periods between the entry of incorrect credentials in order to prevent brute force passwords or denial of service attacks.
Immunity (AV) and Malicious Software
Threat identification - The solution will protect itself from infection by scanning all entered or downloaded data and software for known computer viruses, worms, Trojans and other similar harmful programs.
Threat removal - The solution will be capable of disinfecting or quarantining any file found to contain harmful programs.
Threat alerting - The solution will alert an administrator of any harmful software found during scans.
Threat currency - The solution will regularly (daily or weekly) update the anti-virus definition files.
Innovation – Due to the increased level of innovation in threat creation, the means by which evolving threats will be addressed must be demonstrated.
Intrusion Detection and Protection
Authentication failure – The solution will detect, prevent and record all access attempts which fail identification, authentication or authorisation requirements.
Intrusion notification - The solution will be capable of reporting on all failed access. The application will notify the administrator(s) within 5 minutes of the IPS system triggering alerts.

Innovation – Due to the increased level of innovation in threat creation, the means by which evolving threats will be addressed must be demonstrated.
Physical Access – Where connectivity is provided to end point devices network access controls must be in place to ensure that only authorised and secured endpoints are able to access network resources.
Audit
Audited elements - The business elements that will be audited must be stated explicitly.
Audited fields – The data fields that will be audited must be stated explicitly.
Audit logs – The audit logs should be configurable to record activities appropriate to the system.
Enhanced privileges – A record of all activity by accounts with enhanced privileges must be retained for three months.
Audit status - The solution will collect, organise, summarise and regularly report the status of its security mechanisms.
Security
Data – The solution must be include security measures and controls suitable for holding data up to and including OFFICIAL SENSITIVE, where required.
Disposal – The solution must provide for the secure deletion of any information held on behalf of the customer as the result of the disposal of equipment or change or cessation of the service.
Patching – CQC must be notified when patches or fixes are released for the solution and provided a means to access and apply at short notice any urgent patches resulting from a security exposure. Patching support must be continued for old versions of the software and must be continued for a minimum of two years after the release of a major version that supersedes the prior version. This must be included as part of the support and maintenance costs.
Credentials – The solution must not persist its own user credentials at the presentation or application layer and not persist any external credentials except through the use of tokens.
Authentication and access – The solution shall support 1user account per user. The service shall be demonstrably capable of segregating access to functions and data based on roles for specific users. This must include the ability to control access to create, read, update and delete functions acting on the data objects managed by the software.
Identity & access management
Formal approval of user changes – the solution must provide an audit trail of all user

account and access management actions such as creating, amending and removing.
Account lock out - The number of failed login attempts before system lockout is 5 attempts or less and this value is able to be configured by an administrator.
Database access restrictions - For solutions that have a separate database, such as SqlServer or Oracle, access to the database must be able to be restricted to appropriate and authorised personnel only. For solutions that have a separate database, database accounts and their roles/groups are reviewed periodically for appropriateness. The solution must not use hard coded identifiers or passwords to connect to the database.
Integrity
Integrity - The solution will maintain the integrity of data and have appropriate controls and segregation of access to securely manage data throughout the data lifecycle.
Audit of use – The solution must demonstrate the ability to be configured to generate an accessible log of users' access to data for Create, Read, Update and Delete.
Non-Repudiation
Non-repudiation - The solution will securely segregate and store all data (logs) relating to user actions on the system(s) including: Actions carried out i.e. read, write, change Date and time actions were carried out The identity of the user by unique credentials
Compliance
Legal compliance - Compliance with all UK legislative requirements including the General Data Protection Regulation, the Data Protection Act 2018, the Freedom of Information Act 2000, the Human Rights Act 1998 and any other relevant legislation.
Data purging/archiving - There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.
Certification – The solution should be certified to Cyber Essentials (+) where applicable
Escrow
Source code availability - In the event of buyout or liquidation of the vendor the base source code of the solution must be made available to CQC.
Data centre
Physical damage - The data centre will protect its hardware components from

physical damage, destruction, theft or surreptitious replacement.
Hosting – The system must be hosted by an ISO27001 accredited organisation and must also be demonstrably capable of holding data up to and including OFFICIAL SENSITIVE. Patching must take place in line with the software manufacturer's recommendations and be able to be applied at short notice in the event of a security exposure being identified. This must be included as part of the support and maintenance costs.
Death and injury - The data centre will protect staff from death and injury.
Physical application access - The application will be protected against unauthorised physical access.
Maintenance
System maintenance – System maintenance will not violate any of the security requirements as a result of upgrades or replacement of hardware, software or data.
Additional cloud services requirements
Data ownership - All data remains the property of CQC and may not be used by the contractor except for processing as directed by CQC.
Documentation
Required documentation – The implementation of each security requirement must be documented and approved by named individuals and distributed on an explicit and controlled circulation.

Authority Responsibilities

CQC will appoint a project lead to oversee the work and liaise with / report to supplier contract manager.

Contractor Responsibilities

Appoint a contract manager to oversee the work and liaise with / report to CQC's project lead.

Provide weekly updates of progress (the format of reporting will be agreed at the outset of the contract between the selected supplier and CQC, but it should cover overall progress against plan, risks to plan and mitigating actions, issues and escalations and project budget tracking).

Perform quality assurance on all aspects of the programme.

Provide confirmation that they are managing within the agreed total costs for the project as part of progress updates.

Contract Management and Monitoring

KPIs to be applied to this contract are:

The timeliness of deliverables against key dates

Regular progress reports (weekly)

Working effectively in conjunction with CQC project lead

The selected supplier will be expected to attend a post contract review to consider whether the objectives of the contract were met; to review the benefits achieved; and to identify any lessons learnt for future developments of the system

Testing of system

Training sessions for users

After care support

Indicator	Measured by	Review date/
System availability	99.5% uptime	Quarterly
Page response times	>2 seconds	Quarterly

Timetable

Design to be completed by dates to be agreed

Implementation of system by dates to be agreed

Testing of system by dates to be agreed

Go live date to be agreed.

Skills and Knowledge Transfer

The selected supplier will work closely with CQC's Workplace Facilities and Safety team to ensure the system is designed in line with business needs.

Significant training and guidance required for all staff.

Further Information

The procurement of a case management system is to a limited budget. To minimise costs the selected supplier should consider as far as possible opportunities for joint working with CQC.

Suppliers Response

Android uide 2018

CQC LWS Platform Technical Overview

Schedule 2 - Call-Off Contract charges

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

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 60 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~~ consent of ~~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)
- 5.2 to 5.3 (Force majeure)
- 5.6 (Continuing rights)

- 5.7 to 5.9 (Change of control)
- 5.10 (Fraud)
- 5.11 (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)
- 8.49 to 8.51 (Publicity and branding
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- 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 Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.

2.4 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 and the terms of the Call-Off Agreement, 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 8.83 to 8.91. 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 Accreditation of Information Systems 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/guidance/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 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 - deleted

-

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 8.92 to 8.93 (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 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only Processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional Processing if permitted by Law).

33.2 The Supplier will assist the Buyer with the preparation of any Data Protection Impact Assessment required by the Data Protection Legislation before commencing any Processing (including provision of detailed information and assessments in relation to Processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.

33.3 The Supplier must have in place Protective Measures, details of which shall be provided to the Buyer on request, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier staff with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier's obligations under this Clause;
ii) are subject to appropriate confidentiality undertakings with the Supplier

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

33.5 The Supplier will not transfer Personal Data outside of the European Union unless the prior written consent of the Buyer has been obtained, which shall be dependent on such a transfer satisfying relevant Data Protection Legislation requirements.

33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

33.7 The Supplier will notify the Buyer without undue delay if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation, and insofar as this is possible, in accordance with any timescales reasonably required by the Buyer

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

i) the Buyer determines that the Processing is not occasional;

ii) the Buyer determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

iii) the Buyer determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

33.9 Before allowing any Sub-processor to Process any Personal Data related to this Call-Off Contract, the Supplier must:

i. notify the Buyer in writing of the proposed Sub-processor(s) and obtain its written consent;

ii. ensure that it has entered into a written agreement with the Sub-processor(s) which gives effect to obligations set out in this Clause 33 such that they apply to the Sub-processor(s); and

iii. inform the Buyer of any additions to, or replacements of the notified Sub-processors and the Buyer shall either i) provide its written consent or ii) object.

33.10 The Buyer may at any time put forward a Variation request to amend this Call-Off Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 5 – Guarantee – N/a

~~The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents~~

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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 Data Protection Legislation.
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 □	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing by the Processor under this Call-Off Contract on the protection of Personal Data.
Data Protection Legislation	Data Protection Legislation means: i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; iii) all applicable Law about the processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Takes the meaning given in the Data Protection Legislation.
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	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 RM1557.10 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.
Guarantee	DELETED
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.
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	A 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 but excluding indirect, consequential and special losses 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 Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. 'Process' and 'processed' will be interpreted

	accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
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).
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 Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.

Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - Processing, Personal Data and Data Subjects

[GUIDANCE NOTE TO BUYERS: THE FOLLOWING SCHEDULE IS JUST AN EXAMPLE. YOU MUST CONSIDER HOW DATA PROTECTION LEGISLATION APPLIES TO YOUR SPECIFIC SERVICE AND SUPPLIER AND MUST INCLUDE ANY FURTHER DATA DETAILS IN THIS SCHEDULE WHICH MAY BE REQUIRED TO ENSURE COMPLIANCE WITH THOSE LAWS. FOR EXAMPLE, WHERE THERE MAY BE JOINT CONTROLLERS, DATA SHARING PROVISIONS, ETC. YOU SHOULD ALSO REVIEW THE SUPPLIER'S DATA PROTECTION LEGISLATION TERMS AND CONDITIONS WHICH MAY BE SUFFICIENT IN THEIR OWN RIGHT]

Subject matter of the processing:

[Personal data is stored and used within the Lone Working Solutions Safe Hub platform for providing lone working protection services.

Duration of the processing:

The duration of the processing will be from 25 February 2019 to 24 February 2024

Nature and purposes of the Processing:

To provide Lone worker protection and response services

Type of Personal Data:

Please see table below

[

Categories of Data Subject:

Data Held	Reason for holding	Where data is held	Impact Assessment Risk Category	Data Beach notification
Company Name	Use of the Safe Hub Application Suite and Billing purposes	Secure office filing cabinet, secure restricted Office 365 OneDrive folders, Safe Hub, Sage and Salesforce	Low	ICO
	Marketing	Newsletters/Websites, Case Studies etc	Low	ICO
Contact telephone numbers	Use of the Safe Hub Application Suite and Billing purposes	Secure office filing cabinet, secure restricted Office 365 OneDrive folders, Safe Hub, Sage and Salesforce	Low	ICO
Contact email address	Use of the Safe Hub Application Suite and Billing purposes	Secure office filing cabinet, secure restricted Office 365 OneDrive folders, Safe Hub, Sage and Salesforce	Low	ICO
Contact Address	Use of the Safe Hub Application Suite and Billing purposes	Secure office filing cabinet, secure restricted Office 365 OneDrive folders, Safe Hub, Sage and Salesforce	Low	ICO
Customer Bank details	Billing purposes	Secure office filing cabinet, secure restricted Office 365 OneDrive folders, Safe Hub, Sage and Salesforce	Low	ICO
Safe Hub Lone Worker Name	Use of the Safe Hub Application Suite and Billing purposes	Safe Hub	Low	ICO & Personnel
Safe Hub Lone Worker Mobile Number	Use of the Safe Hub Application Suite and Billing purposes	Safe Hub	Low	ICO & Personnel
Safe Hub Lone Worker Email Address	Use of the Safe Hub Application Suite and Billing purposes	Safe Hub	Low	ICO & Personnel
Safe Hub Lone Worker Gender	Information used by an ARC to identify the Lone Worker in an emergency	Safe Hub	High	ICO & Personnel
Safe Hub Lone Worker Hair Colour	Information used by an ARC to identify the Lone Worker in an emergency	Safe Hub	High	ICO & Personnel
Safe Hub Lone Worker Job Location and Risk Factors	Information used by an ARC to identify the Lone Worker in an emergency	Safe Hub	High	ICO & Personnel
Safe Hub Lone Worker Medical Conditions	Information used by an ARC to identify the Lone Worker in an emergency	Safe Hub	High	ICO & Personnel

Plan for return or destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data:

[Describe how long the data will be retained for and how it will be returned or destroyed]

At the end of the contract all data will be returned to CQC via secure data transfer