Crown Commercial Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	970149233209505
Call-Off Contract reference	con_21112
Call-Off Contract title	Legal Aid Agency CCMS DevOps Managed Service
Call-Off Contract description	Legal Aid Agency CCMS DevOps Managed Service as defined within Schedule 1 – Services
Start date	5 August 2022
Expiry date	4 August 2024
Call-Off Contract value	£1,862,304
Charging method	Monthly in arrears
Purchase order number	TBC

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

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	Secretary of State for Justice, on behalf of the Crown, Ministry of Justice, 102 Petty France, London, SW1H 9AJ
To the Supplier	Capgemini UK plc No. 1 Forge End Woking GU21 6DB Company number: 943935
Together the 'Parties'	

Principal contact details

For the Buyer:

Commercial & Contract Manager

[REDACTED]

For the Supplier:

[REDACTED]

Call-Off Contract term

[REDACTED]

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: ● Lot 3: Cloud support
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: **Schedule 1**

Additional Services	Additional Services can be requested via the Variation Procedure using the G-Cloud12 SFIA Rate Card**.**
Location	The Services will be delivered either from Capgemini offices or remotely at the Supplier's discretion – in either case working practices will be in accordance with Schedule 1 Appendix 2 - Security Management Plan. In exceptional circumstances the Supplier may, at it's discretion, or at the Buyers request attend the offices of the Buyer. Where such request has been made by the Buyer this may incur additional expenses which will be charged to the Buyer on the basis of actuals incurred by the Supplier.
Quality standards	The quality standards required for this Call-Off Contract are detailed in Schedule 1 Appendix 1.
Technical standards:	The technical standards required for this Call-Off Contract are detailed in Schedule 1 Appendix 1.
Service level agreement:	N/A
Onboarding	N/A
Offboarding	The offboarding plan for this Call-Off Contract is detailed in Schedule 8.
Collaboration agreement	At the commencement of this agreement a Collaboration agreement is not required. If during the Term of this contract a Collaboration Agreement is required this will be agreed by both Parties via a Variation to this Call-Off Contract.
Limit on Parties' liability	The annual total liability of either Party for all Property defaults will not exceed £1 million. The annual total liability for Buyer Data defaults will not exceed £1 million or 50% 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 greater of £1million or 50% 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 minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit required by Law ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 14 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: 7.8 to 7.13 Any rights of entry to Supplier premises or other assessments of physical location associated with the audit rights or other obligations in the Call Off Contract shall not apply to Supplier Staff work from home locations.
Buyer's responsibilities	The Buyer is responsible for providing reasonable and appropriate access to their facilities, systems and premises to the Supplier as necessary for them to deliver their obligations under this contract, subject to the appropriate levels of Supplier security clearances (as defined within the Supplier's Security Management Plan) being demonstrated.

	The Buyer shall advise the Supplier of any specific legal and regulatory requirements that are specific to the Buyer and/or CCS to which the Supplier must be aware of to enable it to provide the Services. The Buyer shall ensure that it is entitled to transfer the Buyer Personal Data to the Supplier and/or Approved Subcontractors in full compliance with applicable Data Protection Legislation, including as needed, compliance to any prior required formalities and Data Subject rights, such as information and/or consent when such is required under Data Protection Legislation. The Buyer shall advise the Supplier of the necessary organisational, operational and technological processes that should apply when processing Personal Data. The Buyer shall comply with the Buyer Obligations as detailed in Schedule 1.
Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes: Sufficient and appropriate end user devices necessary for the Supplier to deliver the Supplier's obligations under this Call-Off Contract.

Supplier's information

Subcontractors or partners	N/A
Commercially sensitive information	Details of the Supplier's methodologies, policies and processes. The methodologies, policies and processes remain confidential and commercially sensitive to the Supplier and if such information was disclosed it could be commercially damaging to the Supplier. All information relating to limits of liability, daily fee rates, pricing and charging mechanisms contained in the Call-Off Contract. Disclosure of which may provide affect the Supplier's competitive position. As a result the Supplier considers this information to be a 'trade secret'. The terms of the Supplier's insurance are strictly confidential and if such information was disclosed it could be commercially damaging to the Supplier.

	All details relating to personnel including but not limited to the numbers of Supplier Staff with specific skills, numbers of security cleared staff, staff terms and conditions of employment and staff selection methods are used for the purpose of managing the Supplier Staff to secure trade and generate profit and provides the Supplier with a competitive advantage. If such information was disclosed it could be commercially damaging to the Supplier. Any information relating to other customers of the Supplier that has been obtained as a result of the Services or as a result of procuring the Services (including pre-contract references).

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.

[REDACTED]

Additional Buyer terms

[REDACTED]

1. Formation of contract

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

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

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

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

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

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

Signed	Supplier	Buyer
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Schedule 1: Services

1. Introduction:

The Supplier shall provide the CCMS DevOps Managed Service based on and limited to the Service Profile detailed in Schedule 2 (Call-Off Contract Charges).

The CCMS DevOps Managed Service undertakes the activities selected from the Service Catalogue in Section 3 of this Schedule in accordance with the ways of working stated in Section 2 of this Schedule. The scope of Services shall be provided using the Supplier Staff as set out in the Service Profile and therefore the time spent undertaking the Services will be commensurate with the available Supplier Staff.

2. Ways of Working

The Buyer Product Manager identifies Work Items for the Monthly Work Package from the Product Backlog. Any Work Items identified for inclusion into the Monthly Work Package must be agreed between the Parties. Both new Work Items and any previously agreed Monthly Work Package Work Items will be discussed in the Weekly Service Progress Meeting. Based on a Supplier review, agreed Work Items will either target the current month or future months. The Supplier will then coordinate the delivery of the Monthly Work Package providing updates in the Weekly Service Progress Meeting. The Supplier will work on agreed Monthly Work Package taking into consideration Buyer business priorities, the availability and skills of the Supplier Staff and the status of any external dependencies. Supplier Staff will provide day-to-day updates for any active Work Items via the Agile Board. Any Work Items not completed in the current Monthly Work Package will be carried forward to the next Monthly Work Package.

If no Work Items (that fit within the scope of activities stated in Section 3 of this Schedule) have been identified by the Buyer Product Manager or other factors prevent the Supplier from progressing agreed Monthly Work Package Work Items, the Supplier at its own discretion will progress items from the Product Backlog.

2.1 Background Operational Activities

The Service Catalogue in Section 3 below contains certain business as usual activities (for example performing Incident monitoring). These activities won't be represented on the Agile Board or exist in the Product Backlog, however they will be worked on by the Supplier.

3. Service Catalogue:

Activity	Description	Supplier Output/Outcome	Buyer Obligations

Incident Management	Create, investigate, update & resolve Incident Tickets. Raise and respond to Oracle Support Service Requests. Perform Incident monitoring activities. Attend Incident management related meetings. Where appropriate liaise with CCMS users, internal Buyer teams and Buyer Supplier(s).	Resolved Incident Tickets. Resolved Oracle Support Service Requests.	Raise Incident tickets. Manage major incidents and escalations. Review Incidents tickets and communicate their priority within the JIRA Product Backlog to the Supplier.
Problem Management	Create, investigate, update & resolve Problem tickets. Raise and respond to Oracle Support Service Requests. Attend Problem Management related meetings. Where appropriate liaise with CCMS users, internal MOJ/LAA teams and Buyer Supplier(s).	Resolved Problem Tickets. Resolved Oracle Support Service Requests.	Manage Problems and escalations. Approving changes required as part of problem resolution. Review Problem tickets and communicate their priority within the JIRA Product Backlog to the Supplier.
Maintenance of JIRA Tickets	Create, review, impact & update JIRA tickets in either the JIRA Product Backlog or Agile Board.	Resolved (Definition of Done has been met) JIRA Tickets.	Prioritisation of JIRA Product Backlog. Reviewing JIRA Tickets to ensure Definition of Done has been met.
Knowledge Management	Create & maintain knowledge articles / errors to support CCMS Application Incidents & Problems. As requested by the Buyer, Share knowledge with the Buyer in relation to CCMS Application Incident or Problem (bug) fixes, minor or major enhancements. Share application knowledge with other LAA application teams (such as “Apply and Decide Service”) to assist with design decisions. Provide application and testing knowledge to support the Buyer’s automated testing activity.	Published knowledge articles or known errors.	Provide the mechanisms to allow knowledge articles to be published, stored and distributed.
Release Management	Build CCMS Application code Releases. Document manual configuration Releases. Peer review of code and manual configuration Releases prior to deployment. Deployment of code and manual configuration Releases to Buyer CCMS Application environment.	GitHub Releases (code & configuration), Peer review GitHub Release artifacts, Releases deployed to Buyer CCMS Application environment.	Provision of DBA and Buyer test analyst to assist with Releases where required. Provide sign-off ahead of production Release.

Oracle Application Development	Impact assess and development of CCMS Application changes in relation to Incident or Problem (bug) fixes, minor or major enhancements. Develop CCMS Application changes using GitHub branches to support parallel development.	Create/update documentation in relation to the change to the CCMS Application, as requested by the Buyer. *See Release Management for output in relation to the development.*	Provide detailed requirements & specification documents. Review and sign-off application Design.
Application Software Testing	Perform unit, system, integration and regression testing of the CCMS Application, as agreed with the Buyer.	Test evidence & results	UAT testing. Test acceptance and sign-off. Experienced end-users.
Application Monitoring	Perform CCMS Application specific monitoring using Buyer provided tools and where appropriate escalate any issues and raise supporting Incidents.	Incidents raised for escalated issues that require further investigation.	Perform all infrastructure, database and system software monitoring.
Application Performance Enhancement and Tuning	Investigate CCMS Application performance issues identified by the Buyer and raised as Incidents, and where improvements can be identified and agreed apply code or configuration changes.	*See Release Management for output in relation to changes.*	Provide a suitable environment to perform appropriate analysis.
Service Management	Coordinate the delivery of in-scope activities by the Supplier Staff. Chair a Weekly Service Progress Meeting, held weekly and attended by the Buyer. Provide minutes from the Weekly Service Progress Meeting. Provide Monthly Service Report.	Service Reporting of the KPI' s as defined within Section 4 of Schedule 1. Service Reporting of the following Service Catalogue Supplier Output/Outcomes: Count of Resolved Incident Tickets, Count of Resolved Oracle Support Service Requests, Count of Resolved Problem Tickets, Count of Resolved JIRA Tickets, Count of published knowledge articles or known errors.	Review Monthly Service Report, Attend Supplier Work Package Progress Meeting (held weekly), Review the minutes from the Weekly Service Progress Meeting.

3.1 Additional Buyer Obligations

In addition to the Buyer obligations listed in the table in section 3. above, the Buyer shall:

- Facilitate daily stand-up meetings;
- Support Buyer team development and ways of working
- Undertake the activities stated as those that should be undertaken by the Buyer in Section 2 of this Schedule;

- Provide laptop computers and appropriate software for all Supplier Staff to deliver the Ordered G-Cloud Services;
- Provide the required level of network access and capacity to allow Supplier Staff to fulfil the Ordered G-Cloud Services, during and outside of Service Hours and provide the required Buyer network access, infrastructure, hardware and software;
- Notify the Supplier of any changes to either the Buyer's ICT or security standards which would need to be considered for inclusion into the Security Management Plan.
- Be responsible for all security measures applicable to the Buyer networks and property (including backing up any Buyer software and data), as well as the necessary firewall/security measures (in accordance with the Security Management Plan) to enable the Supplier to deliver the Ordered G-Cloud Services;
- Manage the access to all software, systems and tools (in accordance with the Security Management Plan) to enable the Supplier Staff to deliver the Ordered G-Cloud Services;
- Be responsible for the identification and management of all patching activity across the Buyer's infrastructure and applications, this includes but is not limited to security patching.
- Be responsible for all licensing and Buyer Third Party support contracts required by the Supplier to deliver the Ordered G-Cloud Services;
- Be responsible for providing the resources required to support the Supplier in the delivery of the Ordered G-Cloud Services including but not limited to database administration test resource and support of Provider User Interface (PUI);
- Be responsible for managing the delivery of all aspects required by Buyer Third Parties which impact the delivery of the Ordered G-Cloud Services (example: provision of level 3-4 support from Oracle in respect of Incidents);
- Provide the Supplier with access to the Agile Board and the data required to enable the Supplier to provide on the Performance Indicators stated in Section 4. of this Schedule.
- Review the Monthly Service Report and attend the Service Review Meetings.

4. Performance Indicators:

The Supplier CCMS DevOps Managed Service shall not be subject to any formal service levels. The Supplier shall however measure the following Performance Indicators and report on them in the Monthly Service Report:

4.1. Deployment frequency (count)

- Number of Releases built and ready to be tested by the Buyer
- Number of Releases successfully deployed to the Production Environment

4.2. Lead time for Releases (average lead time)

- Time taken from commencing work to a Release being deployed in the Production Environment

4.3. Release failure rate (percentage)

- The percentage of Releases deployed to Production Environment which result in either regression or fix forward

4.4. Time to restore service (elapsed time for each failure)

- Time taken to recover following a Production Environment Release failure

The Buyer acknowledges that the Performance Indicators above are indicative given that delivery is dependent on activities which are not within the sole control of the Supplier and the measurement tool provided by the Buyer does not allow for this granularity of measurement. These Performance Indicators do not therefore provide a true reflection of the quality or quantity of delivery of the Ordered G-Cloud Services from the Supplier and the Buyer shall have no recourse in respect of these.

5. Service Reporting:

The Supplier shall produce and issue a Monthly Service Report to the Buyer including the following:

- Results of the Performance Indicators described in Section 4 of Schedule 1 Services.
- Monthly Work Package status update (indicating the Work Items completed and outstanding).
- Count of Resolved Incident Tickets.
- Count of Resolved Oracle Support Service Requests.
- Count of Resolved Problem Tickets.
- Count of Resolved JIRA Tickets.
- Count of published knowledge articles or known errors.

Service Review Meetings shall be arranged by the Supplier on an ad-hoc basis as required, no more frequent than once per calendar month.

SCHEDULE 1 APPENDIX 1

STANDARDS AND REGULATIONS

1. **INTRODUCTION**

1.1. This Appendix sets out the Standards and Regulations with which the Supplier shall reasonably comply with in its provision of the Ordered G-Cloud Services. The Buyer shall provide the Supplier with a copy of the technical documents referenced in Section 2 below before the Start Date, including date and version number where applicable. If the Buyer wishes to introduce any new technical documents or make changes to the content of existing documents which impacts on the Supplier's delivery of the CCMS DevOps Managed Service, then this shall be treated as Variation under the Change Control Template in Schedule 9.

2. ENVIRONMENT

2.1. The Supplier undertakes to follow a sound environmental management policy so that its activities comply with all applicable environmental legislation and regulations and that its products or services are procured, produced, packaged, delivered and are capable of being used and ultimately disposed of, in ways that are appropriate from an environmental protection perspective.

2.2. The Supplier warrants that it has obtained ISO 14000/14001 certification for its environmental management and shall comply with and maintain such certification requirements.

2.3. The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2002/96/EC.

SCHEDULE 1 APPENDIX 2

SECURITY MANAGEMENT PLAN

1. INTRODUCTION

1.1 This Appendix covers:

1.1.1 principles of protective security to be applied in delivering the Ordered G-Cloud Services;

1.1.2wider aspects of security relating to the Ordered G-Cloud Services;

1.1.3 the operation, maintenance and continual improvement of an ISMS;

1.1.4 the maintenance of the Security Management Plan;

1.1.5 audit and testing of ISMS compliance with the security requirements;

1.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and;

1.1.7 obligations in the event of actual, potential or attempted Breach of Security.

2. PRINCIPLES OF SECURITY

2.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.

2.2 The Supplier shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:

2.2.1 is in accordance with Good Industry Practice, Law and this Order;

2.2.2 complies with the Security Policy (Schedule 1, Appendix 3);

2.2.3 complies with at least the minimum set of security measures and standards as determined by the Government Functional Standard: GovS 007: Security, version 2.0 dated 13 September 2021 (https://www.gov.uk/government/publications/government-functional-standard-govs-007-security) available from the Cabinet Office Security Policy Division (COSPD)) and https://www.gov.uk/government/publications/government-functional-standard-govs-007-security

2.2.4 meets any specific security threats to the ISMS;

2.2.5 complies with ISO/IEC27001:2013 Standards in accordance with paragraph 5 of this Appendix;

2.2.6 complies with the security requirements as set out in this Appendix.

2.2.7 complies with the Buyer's ICT standards identified by the Buyer and referred to within the Security Management Plan.

2.3 Subject to a Variation and Clause 2.11 of the Supplier Terms, the references to standards, guidance and policies set out in paragraph 2.2 of this Appendix shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

2.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Contract Manager of such

inconsistency immediately upon becoming aware of the same, and the Buyer's Contract Manager shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

2.5 The Supplier shall provide the Ordered G-Cloud Services utilising Supplier Staff or contracted personnel holding BPSS security clearance only.

2.6 Where the Supplier provides the Ordered G-Cloud Services using Supplier Staff falling outside the parameters of this section 2.5 and 2.6, this action will be deemed a Default.

3. ISMS AND SECURITY MANAGEMENT PLAN

3.1 **Introduction**

3.1.1 The Supplier shall provide the Ordered G-Cloud Services in accordance with the Capgemini standard ISMS which is compliant with ISO27001:2013 standards.

3.1.2 The Supplier shall maintain a Security Management Plan in accordance with this Appendix to apply during the Term.

3.1.3 The Supplier shall comply with its obligations set out in the Security Management Plan.

3.1.4 The Security Management Plan shall, unless otherwise specified by the Buyer, aim to protect all aspects of the Ordered G-Cloud Services and all processes associated with the delivery of the Ordered G-Cloud Services, including the Buyer Premises, the Sites, the Supplier System and any ICT, information and data (including the Buyer Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Order.

3.2 **Content of the Security Management Plan**

3.2.1 The Security Management Plan sets out the security measures to be maintained by the Supplier in relation to all aspects of the Ordered G-Cloud Services and all processes associated with the delivery of the Ordered G-Cloud Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Ordered G-Cloud Service comply with the provisions of this Appendix (including the principles set out in paragraph 2.2 of this Appendix. Any amendments to the Buyer's Security Policy which impacts on the Security Management Plan and the Supplier's delivery of the CCMS DevOps Managed Service shall be treated as a Variation under the Change Control Template in Schedule 9.

3.2.2 The Security Management Plan is structured in accordance with ISO/IEC27001, cross-referencing if necessary, to other Appendix of this Order which cover specific areas included within that standard.

3.3 **Amendment and Revision of the Security Management Plan**

3.3.1 The Security Management Plan must be fully reviewed and updated by the Supplier at least annually to reflect:

3.3.1.1 emerging changes in Good Industry Practice;

3.3.1.2 any change or proposed change to the Supplier System, the Ordered G-Cloud Services and/or associated processes;

3.3.1.3 any new perceived or changed security threats; and/or

3.3.1.4 any reasonable request by the Buyer.

3.3.2 On receipt of the results of such reviews, the Buyer will approve any amendments or revisions to the Security Management Plan in accordance with the following:

3.3.3 If any revision of the Security Management Plan made in accordance with paragraph 3.3 of this Appendix, is approved by the Buyer it will be adopted immediately and will replace the previous version of the Security Management Plan. If the Security Management Plan is not approved by the Buyer and the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible, and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the managing disputes clauses 8.68 – 8.71 of the Framework Agreement. No approval to be given by the Buyer pursuant to this paragraph 3.3.4 of this Appendix may be unreasonably withheld or delayed.

3.3.4 Any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a Buyer request or change to this Appendix or otherwise) must be subject to a Variation in accordance with clause 2.11 of the Supplier Terms and must not be implemented until approved in writing by the Buyer.

4. COMPLIANCE WITH ISO/IEC 27001

4.1.1 The Supplier has obtained independent certification of the ISMS to ISO27001:2013 standards and shall maintain such certification for the Term.

4.1.2 If certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27001:2013 standards are not consistent with the Security Policy, and, as a result, the Supplier reasonably believes that it is not compliant with ISO27001:2013 standards, the Supplier shall promptly notify the Buyer of this and the Buyer in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

4.1.3 The Buyer shall be entitled to carry out such regular security audits as may be required, and in accordance with Good Industry Practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001:2013 standards.

4.1.4 If, on the basis of evidence provided by such audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001:2013 standards is not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO/IEC 27001:2013 standards. If the Supplier does not become compliant within the required time then the Buyer has the right to obtain an independent audit against these standards in whole or in part.

4.1.5 If, as a result of any such independent audit as described in paragraph 5.1.4 of this Appendix the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001:2013 standards then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary

compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

4.1.6 be written in plain English; in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule

5. BREACH OF SECURITY

5.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 6.1 of this Appendix, the Supplier shall:

5.2.1 Immediately take all reasonable steps necessary to:

5.2.1.1 remedy such breach or protect the integrity of the ISMS against any such potential or attempted breach or threat; and

5.2.1.2 prevent an equivalent breach in the future.

Such steps shall include any action or changes reasonably required by the Buyer. In the event that such action is taken in response to a breach that is determined by the Buyer acting reasonably not to be covered by the obligations of the Supplier under this Order, then the Supplier shall be entitled to refer the matter to the Variation procedure; and

5.3 as soon as reasonably practicable provide to the Buyer full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security.

SCHEDULE 1 APPENDIX 3

Security Policy

1. Specified in "Ministry of Justice Security Manual" and related documents as provided separately by the Buyer before the Start Date and updated from time to time ("Security Policy" Documents). Any amendments to these Buyer Security Policy documents which impacts on the Supplier's delivery of the CCMS DevOps Managed Service shall be treated as a Variation under the Change Control Template in Schedule 9.

(SECURITY MARKED DOCUMENTATION NOT FOR PUBLICATION)

1.1. The guidance from the Office of the Government SIRO states that protective monitoring data from the Buyer's Protectively Marked ICT Environments is **not suitable** for off shoring and should be stored and processed within the United Kingdom.

1.2. No Supplier activity related to the Ordered G-Cloud Services shall take place outside the United Kingdom, nor Sub-Contracted to a supplier operating outside the United Kingdom.

2. The Supplier will collaborate and co-operate with Buyer Third Parties in the analysis of the CCMS Application relevant Intrusion Detection System (IDS) outputs and alerts as is appropriate and reasonable

3. The Supplier will adhere to all data and information security policies applicable to the CCMS Application provided by the Buyer before the Start Date whilst performing the CCMS DevOps Managed Services.

4. All Supplier Staff with access to CCMS Application code and/or data must be BPSS cleared.

5. Supplier Staff will deliver the Ordered G-Cloud Services as follows:

5.1. Supplier Staff will utilise Buyer supplied devices and the Buyer's network and Buyer provided software services to deliver the Ordered G-Cloud Services within this Call-Off Contract. All aspects of the management (including but not limited to the appropriate security management) of these devices, access to the Buyer's network and software services are wholly the responsibility of the Buyer.

5.2. Supplier Staff may use Supplier resources such as email to facilitate the management and governance of the Ordered G-Cloud Services for sharing for example Supplier documents and Supplier service information however no data held within a CCMS Application will be transferred to or held on Supplier devices.

6. The Supplier shall ensure there is always a named person and/or role from the Supplier, who is accountable for the Supplier's information risk and security management and the Supplier must notify the Buyer of any change as soon as reasonably possible.

7. Assurance

7.1. The Supplier may not utilise Buyer Data or Buyer Systems for purposes other than those permitted by this Agreement and take all proportional measures to ensure the same.

7.2. The Supplier must not Store or Process any Buyer Data outside of the United Kingdom without the prior written consent of the Buyer. The Supplier must declare any existing offshoring to the Buyer and any proposal to offshore, must be discussed and agreed with the Buyer in advance.

7.3. The Buyer will issue a Security Aspects Letter (SAL) to the Supplier, prior to the commencement of the Service, conveying the responsibilities required of the Supplier (and all of their Third Parties), in the handling of Buyer Data,.

8. Risk Assessment & Management

8.1. The Supplier must undertake risk assessment(s) of relevant components, including but not limited to physical locations and supply chain (including all Sub-contractors and Subprocessors), in the provision of the Services.

9. SUPPLIER STAFF SECURITY

9.1. The Supplier is responsible for ensuring that all Supplier Staff (including third parties) must be assured to the UK Government Baseline Personnel Security Standard (BPSS) prior to the ability to directly, or indirectly, access or influence Buyer Systems or Buyer Data.

9.2. Additional Supplier Staff clearances or vetting may be required and will be determined and notified by the Buyer on a case-by-case basis from time-to-time, commensurate with their role and the data they have access to.

9.3. The cost of additional Supplier Staff clearances or vetting is the responsibility of the Buyer and the sponsorship for the same is the responsibility of the Buyer.

10. INFORMATION SECURITY AND ASSURANCE – STANDARDS AND GUIDANCE LOCATIONS

10.1. The table below provides a list of standards the Supplier is required to review and appropriately consider and integrate into their Services.

10.2. This list is correct at the time of issue and may be revised from time to time- by agreement in writing between the parties.

Guidance & Policies	Location	Version (where given)	Dated
Ministry of Justice Data Sharing Principles	link	n/a	22/7/22
Ministry of Justice Security Guidance	link	n/a	22/2/22
APIs and System Integration Standard	link	n/a	11/7/22
Open Standards for Government	link	n/a	16/3/22
UK HMG Technology Code of Practice	link	n/a	10/11/21
Minimum Cyber Security Standard	link	n/a	25/6/18
ISO/IEC 27001:2013	link	Edition 2	Oct 2013
BS10008 (Electronically Stored Information)	link	1:2020	31/5/20
OWASP Top 10	link	n/a	Oct 2021
CPNI Guidance on Physical Security	link	n/a	29/1/21

National Security Vetting Process	link	n/a	31/1/22
National Cyber Security Centre (risk management)	link	Version 1.0	16/11/18
National Cyber Security Centre (CHECK scheme)	link	Version 1.0	10/1/22
National Cyber Security Centre 10 Steps to Cyber	link	Version 1.0	11/5/21
Security Policy Framework	link	n/a	8/2/22

Where n/a represents ‘not available’

Schedule 2: Call-Off Contract charges

The detailed Charges breakdown for the provision of Services during the Term will consist of the following:

The Supplier shall provide the CCMS DevOps Managed Service on a fixed capacity basis, based on the Service Profile detailed in the table below for the duration of the Term. The Supplier may vary the split of roles within the Service Profile to support the Monthly Work Package agreed for a given month.

Service Profile:

[REDACTED]

The CCMS DevOps Managed Service provided will be charged to the Buyer on a Time and Materials basis in accordance with the G-Cloud 12 SFIA Rate Card. The table below provides an estimate of the Charges based on a 19 Working Day month and the Service Profile detailed in the table above.

[REDACTED]

*Services are to be delivered on Working Days. The estimated Charges are based on an average of 19 days per month however the actual number of days provided by the Supplier Staff delivering the Services will fluctuate due to the number of Working Days and Supplier Staff availability in the calendar month. The Charges will therefore be adjusted monthly on the basis of actual time utilised to progress the Monthly Work Package.

Any Additional Services requested by the Buyer which are not in scope of the CCMS DevOps Managed Service will be charged to the Buyer on a Time and Materials basis using the G-Cloud 12 SFIA Rate Card in accordance with the Variation Procedure.

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection
- 8.64 to 8.65 (Severability)

- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- 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:

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

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'

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

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

5.1.4 have entered into the Call-Off Contract relying on 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 portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

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

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. 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:

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

11.5.2 Supplier’s performance of the Services

11.5.3 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:

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

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

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

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

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

11.7.3 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:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

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

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

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

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

13.6.6 buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

18.2.2 Call-Off Contract Charges paid during the notice period 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:

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 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:

21.6.1 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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 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:

24.1.1 Property: for all Defaults by either party 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

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, 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:

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

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

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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:

29.6.1 its failure to comply with the provisions of this clause

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

29.7 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:

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement – NOT APPLICABLE

Schedule 4: Alternative clauses – NOT APPLICABLE

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 8.12 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995

- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions
b. men and women or married and unmarried persons
c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
f. persons of different ages
g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

a. the issue of written instructions to staff and other relevant persons
b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters

d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or

B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee – NOT APPLICABLE

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Agile Board	means the board (for example Kanban Board) displaying CCMS Application JIRA tickets.
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 IPR Software	means any software created by the Supplier (or by a third party on behalf of the Supplier, including by any Subcontractor) specifically for the purposes of this Order.

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.
Buyer Third Parties	means the companies that provide services to the Buyer, in relation to CCMS Application this includes the infrastructure provider (supplying hardware and software services) and third parties (Banks, cash collections, EDRMS, central print, benefit checker and debt recovery).
Buyer System	means the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Order which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Ordered G-Cloud Services.
Buyer Premises	means premises owned, controlled or occupied by the Buyer or any body of the Crown which are made available for use by the Supplier or its Subcontractors for provision of Ordered G-Cloud Services (or any of them) on the terms set out in this Order or any separate agreement or licence.
Breach of Security	means in accordance with the security requirements in Schedule 1 Appendix 3 and the Security Policy, the occurrence of: any unauthorised access to or use of the Ordered G-Cloud Services, the Buyer Premises, the Sites, the Supplier System and/or any ICT, information or data (including the Buyer Data) used by the Buyer and/or the Supplier in connection with this Order; and/or the loss and/or unauthorised disclosure of any information or data (including the Buyer Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Order.
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.

CCMS Application	means the Client and Cost Management System application, including all related CCMS interfaces.
CCMS DevOps Managed Service	means the services provided by the Supplier under this Call-Off Contract as detailed in Schedule 1
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').
Contract Change Note (CCN)	means the contract change note specified in Schedule 9.
Contract Change Procedure	means the contract change procedure specified in section 32 (Variation Process) of the Supplier Terms and the Contract Change Template in Schedule 9.
Contract Manager	means the Buyer Representative and Supplier Representative nominated and notified to the other Party at Start Date and amended as notified from time to time.
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.

Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Daily Stand-Up Meeting (DSUM)	The Daily Stand-Up Meeting (DSUM) is one of the Agile Ceremonies arranged by the Buyer and attended by the Supplier during which the Parties report and discuss updates in relation to items on the Agile Board.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) 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 GDPR
Days	means calendar days.
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.

Definition of Done	means the set of items that must be completed before a JIRA ticket is considered finished.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Exit and Service Transfer Arrangements	means the arrangements set out in Schedule 8 which will apply on the Expiry Date or in the event of the Ending including partial Ending (howsoever arising) of this Order.

Exit Plan	means the plan produced in accordance with paragraph 2 of Schedule 8 by the Supplier to be agreed by the Buyer to facilitate any transfer of the Ordered G-Cloud Services (or any part of the Ordered G-Cloud Services), for whatever reason, from the Supplier or any Subcontractor to the Buyer or to a Replacement Supplier.
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 RM1557.12 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.
G-Cloud 12 SFIA Rate Card	means the rate card from which additional Supplier Staff will be charged to the Buyer
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
ICT Environment	means the Buyer System and the Supplier System.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Incident	means an unplanned interruption to the delivery of an IT service, a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an Incident.

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.
Service Profile	means the Supplier Service Profile as detailed in Schedule 2 (Call-Off Contract Charges)
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.

IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
ISMS	means the Information Security Management System as defined by ISO/IEC 27001. The scope of the ISMS will be as agreed by the Parties and will directly reflect the scope of the Ordered G-Cloud Services
ITIL	means a set of best-practice publications for IT service management. Owned by the Cabinet Office (part of HM Government), ITIL gives guidance on the provision of quality IT services and the processes, functions and other capabilities needed to support them. The ITIL framework is based on a service lifecycle and consists of five lifecycle stages (service strategy, service design, service transition, service operation and continual service improvement).
JIRA	means Agile software tool used to track issues using tickets. JIRA tickets are held in either the Product Backlog or the Agile Board.
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.
Knowledge Management	Activity as defined within Section 3 Service Catalogue. Maintenance of sharing day-to-day operational knowledge required to support the CCMS Application.
Knowledge Transfer	means activities designed to impart detailed information regarding the CCMS Application from Supplier to Buyer and is managed within an agreed exit plan.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.

Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
Monthly Service Report	means the report produced by the Supplier each month on the CCMS DevOps Managed Service.
Monthly Work Package	means the Work Items targeted for delivery by the Supplier (during the Weekly Service Progress Meeting) in the calendar month.
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.
Out of Hours Release	means Code deployment to production CCMS Application environment outside Service Hours
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.
Oracle Support Service Request	means a support ticket raised to progress any out-of-the-box software issue with the Buyer's Supplier Oracle.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Performance Indicators	means the measures that the Supplier will report on to the Buyer in the Monthly Service Report. These are for information only and are not subject to service credits.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Problem	means a cause of one or more Incidents. The cause is not usually known at the time a Problem is created and the Problem Management process is responsible for further investigation.
Problem Management	means the process responsible for managing the lifecycle of all Problems.
Processing	Takes the meaning given in the GDPR.

Processor	Takes the meaning given in the GDPR.
Product Backlog	means the backlog of JIRA tickets that detail new functionality, enhancements, bug fixes and other activities relating to be CCMS Application.
Product Manager	Agile role (performed by the Buyer) whose responsibility it is to provide a bridge between the CCMS Application Buyer stakeholders and the Agile team. The Product Manager is also responsible for defining the product roadmap, assessing business value, and prioritising the Product Backlog.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
Protectively Marked	has the meaning as set out in the Security Policy Framework.
Provider User Interface (PUI)	means the custom-built web application which is developed, maintained and supported by the Buyer.

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.
Release(s)	means the packaged CCMS Application code or manual configuration changes which are to be deployed into CCMS Application environments.
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).
Scrum Master	Agile role whose purpose is to facilitate and ensure that the scrum framework is followed.
Security Management Plan	The Supplier's security management plan (current version number 2.2 dated February 2017 or any subsequent versions) developed by the Supplier in accordance with clause 16.1 and approved by the Buyer.
Security Policy	means the Buyer's security policy which is set out in Schedule 1 Appendix 3, as updated from time to time.
Security Policy Framework	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division).
Services	The services ordered by the Buyer as set out in the Order Form.

Service Catalogue	means the catalogue of activities which the Supplier may perform on behalf of the Buyer, as detailed in the table in Schedule 1.
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 Hours	means 8am to 6pm UK standard time on Working Days.
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.
Service Review Meeting	means the meeting held between the Supplier and Buyer as required on an ad-hoc basis to discuss performance of the CCMS DevOps Managed Service.

Service Transfer	means any transfer of the Ordered G-Cloud Services (or any part of the Ordered G-Cloud Services), for whatever reason, from the Supplier or any Subcontractor to the Buyer or to a Replacement Supplier.
Sites	means any premises from which Ordered G-Cloud Services are provided or from which the Supplier manages, organises or otherwise directs the provision or the use of Ordered G-Cloud Services or where any part of the Supplier System is situated or where any physical interface with the Buyer System takes place.
Software	means any Buyer IPR Software, Supplier Software and Third Party Software.
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
Standards and Regulations	means the standards and regulations as set out in Schedule1 Appendix 1 with which the Supplier will comply in the provision of the Ordered G-Cloud Services and its responsibilities and obligations hereunder.
Start Date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.

Supplier Equipment	means the hardware, computer and telecoms devices and equipment supplied by the Supplier or its Sub-Contractors (but not hired, leased or loaned from the Customer) for the provision of the Ordered G-Cloud Services.
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.
Supplier System	means the information and communications technology system used by the Supplier in providing the Ordered G-Cloud Services including the Software, the Supplier Equipment and related cabling (but excluding the Customer System).
Term	The term of this Call-Off Contract as set out in the Order Form.
Ticket	means either an Incident or Service Request raised by the Buyer Service Desk.
Third Party Software	means software which is proprietary to any third party other than an Affiliate of the Supplier which is or will be used by the Supplier for the purposes of providing the Ordered G-Cloud Services.
Value Added Tax (VAT)	means value added tax as provided for in the Value Added Tax Act 1994 and any other applicable sales tax.
Variation	This has the meaning given to it in clause 32 (Variation process).
Weekly Service Progress Meeting	means the weekly meeting chaired by the Supplier and attended by the Buyer to review and agree Monthly Work Package Work Items. During the meeting the Supplier will also share progress updates on the previously agreed Monthly Work Package Work Items.
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.

Work Item	means an activity in the Service Catalogue undertaken by the Supplier.
Year	A contract year.

Schedule 7: GDPR Information

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

Annex 1 - Processing Personal Data

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

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

1.2 The contact details of the Supplier's Data Protection Officer are:
[REDACTED]

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

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is the Controller and the Supplier is the Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: The Buyer provides civil and criminal legal aid and advice in England and Wales to help people deal with their legal problems and holds Personal Data in respect of these. In addition, the Buyer holds Personal Data regarding their employees, suppliers and third parties. The Supplier is providing Services in support of systems which provide payments and receive monies to and from solicitors and clients and will need to process this Personal Data in order to provide the Services under this Call-Off Contract.
Duration of the Processing	For the duration of the Call-Off Contract Term.
Nature and purposes of the Processing	Storage and retrieval of Personal Data on Buyer provided IT using secure connections to the Buyer's network, and in accordance with the Buyer's reasonable instructions notified to the Supplier. The Supplier will use the appropriate organisational, operational and technological processes provided by the Buyer to the Supplier. In order to provide the Services under this Call-Off Contract to the Buyer the Supplier is able to use the Buyer's Personal Data to undertake the following activities: ● View, analyse & debug Personal Data ● Run reports to review specific Personal Data elements

	● Develop/customise programs to produce letters/data files incorporating Personal Data ● Develop and run regular and ad hoc batch schedules to enable Personal Data to be saved and approved (modified and updated) ● Provide guidance to the Buyer on removal of duplicated or problematic Personal Data ● Assist with the development of interfaces from/to third party products which may incorporate Personal Data ● Manipulation of data files which contain Personal Data under instruction of the Buyer
Type of Personal Data	● Full name ● Home address ● Business address ● Date of birth ● Gender ● Marital status ● NI number ● Telephone number(s) ● Email address Details of individual legal aid clients and (where relevant) their partner's financial circumstances which may include: • Bank account numbers, sort code and account balances • Details of financial transactions • Details of employment status • Details of benefit claims and financial support and assistance • Details of debts • Details of property, vehicles and other capital assets Details of legal proceedings in relation to individual legal aid clients and their opponents including: • Nature and type of case • Court hearing the case and hearing dates • Narrative details of proceedings, including witness statements, legal counsel opinion and evidence Details of legal aid providers including: • Name(s) of staff members • Business email addresses of provider staff members • Business phone numbers of provider staff members • Account numbers (unique identifiers) for provider staff members Details of MoJ employees including: • Names • Business email addresses • Username • Audit records detailing actions taken on the Buyer system
Categories of Personal Data	To complete the purposes defined above the Supplier will process personal data, special category data, criminal offence data and children's data contained in the Buyer's System.

Categories of Data Subject	All categories of data may be processed in respect of legal aid clients, their partners, children and other individuals associated with proceedings. Basic Personal Data only may be processed in respect of MoJ Employees and MoJ contractors, including legal aid providers holding a legal aid contract or instructed by a legal aid provider.
Special Categories of Personal Data	The following types of special category data may be processed in respect of individual legal aid clients, their partners, children and other individuals associated with proceedings. ● personal data revealing racial or ethnic origin; ● personal data revealing political opinions; ● personal data revealing religious or philosophical beliefs; ● personal data revealing trade union membership; ● genetic data; ● data concerning health; ● data concerning a person's sex life; and ● data concerning a person's sexual orientation.
Criminal Offence Data	Narrative information contained in the Buyer's System may detail allegations, investigations, charging details, convictions, court penalties/sentences relating to individual legal aid clients, their partners, children and other individuals associated with proceedings.
Children's Data	The Buyer's System contains personal information of the types detailed above relating to children where they are either a legal aid client, or a party to proceedings of a legal aid client.
Plan for return and destruction of the data once the Processing is complete	At the end of the Call-Off Contract Term, the Supplier must return any Buyer equipment on the last day of the Contract.

Annex 2: Joint Controller Agreement – Not Required

Schedule 8: Exit and Service Transfer Arrangements

These terms are supplemental to clauses 21. and 22. within the Call-Off Contract Part B: Terms and Conditions.

1. Introduction:

1.1. This Appendix describes the duties and responsibilities of the Supplier to the Buyer leading up to and covering the Expiry Date or Ending (howsoever arising) (including partial Ending) of this Order and the transfer of service provision to a Replacement Supplier.

1.2. The objectives of the exit and Service Transfer arrangements are to ensure a smooth transition of the availability of the Ordered G-Cloud Services from the Supplier to the Buyer or a Replacement Supplier at the Ending (howsoever arising) (including partial Ending) or at the Expiry date as stated within PART A: Order Form.

2. Exit Plan:

2.1. No later than six(6) months after the Start date as stated within Part A: Order Form, and thereafter as specified in paragraph 2.3 of this Appendix, the Supplier shall prepare an updated Exit Plan for review by the Buyer. The Buyer shall review the Exit Plan within twenty (20) Working Days of receipt from the Supplier and shall notify the Supplier of any suggested revisions to the Exit Plan. In this respect, the Buyer will act neither unreasonably, capriciously nor vexatiously. Such suggested revisions shall be discussed and resolved within ten (10) Working Days. The agreed Exit Plan shall be signed as approved by each Party.

2.2. The Exit Plan shall provide comprehensive proposals for the activities and the associated liaison and assistance that will be required for the successful transfer of the Ordered G-Cloud Services, including the following details:

2.2.1. scope, critical success factors and objectives;

2.2.2. Buyer and Supplier obligations (in accordance with section 5.7 of the Supplier Terms);

2.2.3. key assumptions of the exit;

2.2.4. proposal for exit requirements, timelines and work-streams;

2.2.5. proposal for exit governance, including Supplier and Buyer key responsibilities, acceptance criteria and meetings/reporting; and

2.2.6. a proposal for risk and issue management during exit.

2.3. The Supplier shall provide a revised version of the Exit Plan to the Buyer 3 months prior to the Expiry Date. The revised Exit Plan shall be reviewed and agreed in accordance with the provisions of paragraph 2.1 of this Appendix.

2.4. Any additional Exit Plan required outside of that described in section 2. of this Schedule, shall be chargeable to the Buyer.

3. Assistance on Expiry or Ending:

3.1. In the event that this Order expires or Ends the Supplier shall, where so requested by the Buyer, provide assistance to the Buyer to migrate the provision of the Ordered G-Cloud Services to a Replacement Supplier as set out in the Exit Plan. These activities will be chargeable as set out in section 9.4 of the Supplier Terms.

4. Pre-Service Transfer Obligations:

4.1. This will be handled in accordance with Clause 29 of Part B and section 5.7 of the Supplier Terms.

5. Application of Tupe on a Service Transfer:

5.1. This will be handled in accordance with Clause 29 of Part B and section 5.7 of the Supplier Terms.

6. TUPE Indemnities:

This will be handled in accordance with Clause 29 of Part B and section 5.7 of the Supplier Terms.

Schedule 9: Change Control Template

1. Introduction:

1.1. This Appendix sets out the Contract Change Note to be used by the Buyer and the Supplier to effect Variations to this Order.

2. Procedure:

2.1. Should either Party wish to propose a contractual Variation to this Order or require additional work, that Party shall submit a Contract Change Note detailing the proposed action to the other Party using the template at Schedule 9 (or an agreed updated template) in accordance with clause 2.11of the Supplier Terms.

Contract Change Note for the Contract Change Procedure

Sequential Number: [to be allocated by the Buyer]

Title: .....

Originator: ..... for the [Supplier]

Date change first proposed: .....

Number of pages attached: .....……

WHEREAS the Supplier and the Buyer entered into an Order for the provision of the Ordered G-Cloud Services dated [date] and now wish to amend that Order as follows:

Reason for proposed change

[Party proposing change to complete]

Full details of proposed change

[Party proposing change to complete]

Details of likely impact, if any, of proposed change on other aspects of the Order

[Party proposing change to complete]

IT IS AGREED as follows:

1. With effect from [date] the Order shall be amended as set out below:
   [Details of the amendments to the Order to be inserted here – to include the explicit changes required to the text in order to effect the change, i.e. Clause/Schedule/Appendix/paragraph number, required deletions and insertions etc]
2. Save as herein amended, all other terms and conditions of the Order inclusive of any previous Contract Change Notes shall remain in full force and effect.

Signed for and on behalf of the Supplier

By .....

Name .....

Title .....

Date .....

Signed for and on behalf of the Buyer

By .....

Name .....

Title ……..……..

Date .....