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	(Access Expense) 3988 6092 6793 187
Call-Off Contract reference	CON_XXXX
Call-Off Contract title	Judicial Fees and Expenses System for HMCTS
Call-Off Contract description	The Buyer is purchasing licenses for the use of the Services better described herein, as offered by the Supplier on the G Cloud digital marketplace.
Start date	17/02/2021
Expiry date	16/02/2023
Call-Off Contract value	£ 443,911.96
Charging method	BACS transfer
Purchase order number	To be confirmed upon contract signature

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	The Secretary of State for Justice on behalf of Her Majesty's Courts and Tribunals Service The Ministry of Justice 102 Petty France London SW1H 9AJ
To the Supplier	Access UK Limited 0845 345 3300 The Old School Stratford St Mary Colchester CO7 6LZ United Kingdom Company number: 2343760
Together the 'Parties'	

Principal contact details

For the Buyer:
[REDACTED]

For the Supplier:
[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 17th February 2021 and is valid for up to 24 months.

Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for two period(s) of up to 12 months each, by giving the Supplier one month written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

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

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

G-Cloud services required	The Services the Supplier will provide as part of this Call-Off Contract include items below: • Suite of standard reports, including: o Dimensions Reporting o Expenses Reporting o Insight Reporting o Pension Data Reports o Functionality to extract data for reporting o Reporting will follow the data exporting format of one or more of the following formats: csv; xlsv; xls; delimited text. • Premium Level Support from a designated Relationship Manager to work with HMCTS on behalf of the Buyer • Consultancy software development, including scoping and write up, software development, acceptance user testing and go live. • Functionality for upload of Receipts and other documents. • Accounting information relevant to Office Holder fees and expenses claims, including HMCTS cost centres and General Ledger expense codes embedded into the system • Ability for Finance team to access individual claims, quality assure and reject any items outside of fees and expenses policy • Option to embed claim limits in line with fees and expenses policy • Full VAT management • Functionality for submission of Mileage Claims, including a mileage calculator
Additional Services	1. Additional Services: Please include the following wording in this section: Customer Success Plan: Premier Plan Details of this plan can be found here: https://pages.theaccessgroup.com/rs/302-WOS-863/images/DataSheet_CustomerSuccessPlans_2020_07_01_V6.pdf as found in the Supplier Terms. This includes the following services: • Service Support is offered via web chat, telephone and Live Chat. Service Support hours for these three services is 8am – 6pm, Monday – Friday (excluding Bank Holidays). • The Supplier will provide a Named Technical Support Engineer to the Buyer. • Up to 8 Buyer Users may raise a support case • Customer Success Portal for Unlimited number of Buyer users • Task Based Advice and Guidance from the web, telephone and the Named Technical Support Engineer • Designated Customer Success Manager • Product Group Roadmap Briefings • VIP Treatment at Access World

	• Tailored Success Action Plan - jointly agreed set of objectives to ensure you're getting the best return on your investment in the Access technology • Monthly Customer Success Reviews • Tailored Success Action Plan • Proactive Case Management – making sure cases are progressed, working with support managers and development teams to facilitate a resolution. • Proactive Advice and Guidance – delivered either by themselves or by connecting you with other experts through success days/points. • Product updates – keeping you abreast of new functionality that may be pertinent to your business. • Customer Advocate - being your advocate in Access, to answer any queries or to connect you with the right resources.
Location	Where relevant, the Services will be delivered to the Buyer's address as detailed in Part A of the Order Form.
Quality standards	**Staff Security** The Government security clearance shall be Up to Baseline Personnel Security Standard (BPSS). **Asset Protection** Knowledge of data storage and processing locations: Yes Data storage and processing locations: United Kingdom User control over data storage and processing locations: No Datacentre security standards: Complies with a recognised standard (for example CSA CCM version 3.0) Penetration testing frequency: At least once a year Penetration testing approach: 'IT Health Check' performed by a Tigerscheme qualified provider or a CREST-approved service provider Protecting data at rest:

	• Physical access control, complying with another standard • Encryption of all physical media Data sanitisation process: Yes Data sanitisation type: Explicit overwriting of storage before reallocation Equipment disposal approach: Complying with a recognised standard, for example CSA CCM v.30, CAS (Sanitisation) or ISO/IEC 27001. **Standard and Certifications** ISO/IEC 27001 certification: Yes Who accredited the ISO/IEC 27001: ISOQAR ISO/IEC 27001 accreditation date: 25/08/2017 What the ISO/IEC 27001 doesn't cover: Nothing is excluded from the Standard
Technical standards:	**Operational Security** The Supplier shall ensure, and provide evidence to the Buyer, that all security requirements – functional and non-functional – applicable to the contractor, will flow down in the supply chain and will apply to all sub-contractors, Partners, and suppliers that participate in this contract. The Supplier will abide by the following Operational Security Requirements throughout this contract: 1. Vulnerability Managed Approach - Conforms to CSA CCM v3.0 a. Patched and audited by the Supplier's patch management system. All non-critical OS patches are applied within one calendar month of release, first into pre-production and then into production, as part of the scheduled maintenance window. b. AV Updates - Signatures are updated hourly. / Rules are reviewed at minimum every 3 months. Logs are reviewed at minimum every 3 months. c. Access staff responsible for the maintenance of our hosting services subscribe to industry newsletters,

	belong to various security forums and we additionally receive notifications from our vendors. 2. Protective Monitoring Approach – Conforms to CSA CCM v3.0 a. traffic monitoring and content-based alerting which alerts on changes to the site and/or traffic flows implemented at infrastructure and application level. The Supplier shall proactively monitor third party suppliers (hardware, OS, application/web and database server software) vulnerability reporting and security fix availability. b. Any vulnerabilities found and fixes provided by third party suppliers are patched by our infrastructure team in a timescale appropriate for their level of severity. c. Any penetration test findings are fixed by Development in a timescale appropriate for their level of severity. 3. Incident Management Approach a. The Supplier will operate a robust incident management process in line with ISO27001:2013. b. The requirements for support are as per those available for Access Premier Success Plan which are detailed at page 6 of this contract. c. HMCTS Bristol Finance Team Members will report all incidents using a pre-defined process using the online Access Support Portal https://access-support.force.com/Support/s/login/ d. Incident reports will be provided in writing by the Supplier to the Buyer following forensics and closure. Reports will be sent to Buyer's Principal Contact and copied to HMCTS Finance Support Centre Manager. Reports will explain the causes of the incident; the steps taken to rectify the immediate issues created by the incident; and, mitigating actions to be taken to ensure that the incident does not recur. Reports on P1 incidents will be provided within a week; P2 and P3 reports within 2 weeks. A written report shall contain the following information (but not exclusively): i. the cause of the incident ii. the resolution of the incident the ongoing mitigation actions to prevent future incidences

Service level agreement:	The service level and availability criteria required for this Call-Off Contract are found here: https://www.theaccessgroup.com/media/29858/saas-sla-v2.pdf the content of which has been replicated below, for ease of reference: SaaS SLA 1. Overview This Schedule represents an availability service level agreement between You and Us in respect of the SaaS. 2. SaaS parameters The following service parameters are Our responsibility in the ongoing support of the SaaS: 2.1 Availability We will use commercially reasonable efforts to make the SaaS available 24 hours a day (for at least 99.8% of the time per calendar year), seven days a week, except for unavailability during emergency or routine maintenance. You acknowledge and accept that Your access to the internet cannot be guaranteed and that We are not liable for deficiencies in Your own internet connections or equipment and that We are entitled to take measures that affect accessibility to the SaaS where We consider it to be necessary for technical, maintenance, operational or security reasons. You are responsible for ensuring that Your internet connections, computer unit and telephone solutions are compatible with the SaaS and for any damage that may be caused to such items by anything You access or obtain using them. We shall not be liable for any losses suffered by You as a result of any such incompatibility or damage. You are responsible for paying any and all charges in

relation to Your internet connection, computer unit and telephone service.

2.2 Priority Definitions

Incidents logged with customer support will be prioritised as follows:

PRIORITY	RESPONSE TIME	TARGET RESOLUTION TIME	BUSINESS HOURS	DEFINITION
	SaaS			
1	30 minutes	4 hours	24 hours daily	Complete outage
2	1 hour	8 hours	Working Hours	Service degraded but useable
3	1 day	3 days	Working Hours	Non-service impacting
4	3 days	10 days	Working Hours	Non urgent and impacting

2.3 Maintenance windows

We reserve the right to take the SaaS offline in order to carry out emergency maintenance but will endeavour to give you as much

notice as reasonably possible. Routine maintenance, which may also require the SaaS to be taken offline, will be carried out during

scheduled windows and may require the service to be brought down for monthly maintenance, patching upgrades and infrastructure

changes. These service interruptions will be scheduled to take place on the third Wednesday of every month between 2200 and 0400

GMT.

Updates and upgrades are performed at our discretion. You will be informed of all planned upgrades with a minimum 1 week’s notice.

2.4 Server and data back-up and recovery

All servers used to provide the SaaS are subject to Our current back-up and recovery procedures. Sufficient hardware is available to

ensure continuity of service in event of total server failure with a target recovery time of [12] hours for any given server.

Backup policy and retention is:

(a) All backups are stored on disk within a multi tenancy data vault at our DR Datacentre and encrypted.

	(b) Data retention for all backups is 90 Days (c) Virtual Machine images are kept for 7 days using Veeam, backed up once a day from 2200GMT, 7 days per week.. (d) SQL Backups are transactional, taken every 15 minutes and full daily, regardless of user activity. 2.5 Server monitoring All servers used to provide the SaaS are monitored by or on behalf of Us.
Onboarding	The services described herein have been implemented. No further onboarding is required.
Offboarding	Should the Buyer give sufficient notice to serve termination on the contract, the Supplier will provide the data held within the system as per below: • Confidential Information belonging to the Buyer shall promptly, and in any event within 30 days, be returned to the Buyer upon written request • Buyer Data will be returned in accordance with Schedule 7, or alternatively, at the Buyer's written instruction. The Buyer must allow the Supplier a reasonable timeframe for adhering to instructions outside of those set at Schedule 7
Collaboration agreement	Not applicable.

Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed £300,000.00. The annual total liability for Buyer Data Defaults will not exceed £250,000.00 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other Defaults will not exceed the greater of £250,000.00 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £10,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £10,000,000 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 60 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: 7.6 The Supplier's records and accounts will be kept until the latest of the following dates:

	7.6.1 7 years after the date of Ending or expiry of this Framework Agreement 7.6.2 7 years after the date of Ending or expiry of the last Call-Off Contract to expire or End 7.6.3 another date agreed between the Parties 7.7 During the timeframes highlighted in clause 7.6, the Supplier will maintain: 7.7.5 proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Framework Agreement; 7.7.6 records of its delivery performance under each Call-Off Contract, including that of its Subcontractors. 7.8 CCS will use reasonable endeavours to ensure that the Audit does not unreasonably disrupt the Supplier, but the Supplier accepts that control over the conduct of Audits carried out by the auditors is outside of CCS's control. 7.9 Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to: 7.9.1 provide audit information without delay 7.9.2 provide all audit information within scope and give auditors access to Supplier Staff 7.10 The Supplier will allow the representatives of CCS, Buyers receiving Services, the Controller and Auditor General and their staff, any appointed representatives of the National Audit Office, HM Treasury, the Cabinet Office and any successors or assigns of the above access to the records, documents, and account information referred to in clause 7.7 (including at the Supplier's premises), as may be required by them, and subject to reasonable and appropriate confidentiality undertakings, to verify and review: 7.10.1 the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement) 7.10.3 the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier 7.10.4 any other aspect of the delivery of the Services including to review compliance with any legislation

	7.10.5 the accuracy and completeness of any MI delivered or required by the Framework Agreement 7.10.6 any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records 7.10.7 the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date 7.13 Each Party is responsible for covering all their own other costs incurred from their compliance with the Audit obligations. Where the Buyer is required by law to carry out an audit on the Supplier, such audit will be subject to the following conditions: • The Buyer shall use all reasonable endeavours to minimise the frequency and duration of any audit
Buyer's responsibilities	The Buyer is responsible for: • Provision of a full specification for the data • Provision of project manager and/or project sponsor • Provision of accurate, consistent data for all users • Reviewing resource activities and deliverables and approving all properly raised invoices for work against tasks and deliverables *in line with the Assurance process agreed between the Buyer and the Supplier in Schedule 1 of this Call-Off Contract document.* • Providing the Supplier with the appropriate level of access to the Buyer's business and technical environments necessary for the Supplier to deliver the Services • Working with the Supplier in order that any required resources, documentation, and access to relevant sites will be made available to support the achievement of activities and production of deliverables according to the Implementation Plan • Provision of data deemed relevant to the configuration of the Access systems

	• Compliance with any other reasonable instruction or request given by the Supplier
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	[REDACTED]

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS transfer
Payment profile	The payment profile for this Call-Off Contract is **that** invoices will be sent to the Buyer monthly in arrears. Where the Charges are expressed as Consulting Services, such fees are invoiced upon completion of the works carried out and are payable by the Buyer within 30 days by the chosen payment method.

	Unless expressly agreed otherwise between the parties, expenses incurred by the Supplier as a result of carrying out the Consulting Services shall be charged back to the Buyer at cost (without mark-up). The Supplier's expense policy is as follows: **Access Expenses Policy** Overnight stays are necessary if otherwise a Consultant would need to leave home before 7am and/or arrive home after 8pm, or where it is economic to stay over, or unreasonable to travel home We always source and use hotels with a corporate rate (e.g., Premier Inn) e.g., up to £80 per night or £120 per night in central London Breakfast up to £8, Evening Meal up to £20 when staying away Flights and Trains recharged at cost. Standard Class for travel less than 6 hours Mileage broadly HMRC guidelines currently 50p per mile (depends on engine size & type & car allowance etc)
Invoice details	The Supplier will issue electronic invoices to reflect the payment profile outlined above. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice. All invoices must include enough detail reasonably expected for a Buyer to be able to identify for what software and/or services the invoice relates. To enable successful processing, all invoices submitted to MoJ must clearly state the word 'invoice' and contain the following: • a unique identification number (invoice number) • your company name, address and contact information • the name and address of the department/agency you're invoicing • a clear description of what you're charging for • the date the goods or service were provided (supply date) • the date of the invoice • the amount(s) being charged • VAT amount if applicable • the total amount owed • a cost centre code (available from your MoJ business contact) or a valid purchase order (PO) number If any of the above information is missing from your invoice, it will be returned to you

Who and where to send invoices to	Invoices will be sent to Email: APinvoices-CTS-U@gov.sscl.com Copies are to be sent to [REDACTED]
Invoice information required	All invoices must include enough detail reasonably expected for a Buyer to be able to identify for what software and/or services the invoice relates.
Invoice frequency	Invoice will be sent to the Buyer to reflect the payment profile.
Call-Off Contract value	The total value of this Call-Off Contract is £443,911.96
Call-Off Contract charges	The breakdown of the Charges can be found at Schedule 2. [REDACTED] Consultancy services are called off by the Buyer (HMCTS) when required. The Buyer will agree consultancy work to be carried out and will advise the Supplier of required consultancy work. The Supplier will provide the Buyer with a quote outlining the total number of hours required to complete this work, and the total charges for this consultancy work using the fixed rate per hour as per the Call-Off Contract. The hourly Consultancy rate under the quote for consultancy work provided by the Supplier will not exceed the Consultancy hourly rates agreed under this Call-Off Contract. The Buyer will agree the quoted time and charges for this consultancy work, and notify the Supplier of this agreement, in advance of any quoted consultancy work taking place by written notice. Only once the Buyer has provided confirmation to undertake this consultancy work to the Supplier by written notice (an email is accepted as 'written notice') may this consultancy work be completed by the Supplier. Where the Buyer has a requirement for any additional consultancy services from the Supplier, the Buyer will make the Supplier aware of these additional consultancy service requirements (as per the Assurance process above). The Supplier will provide the Buyer with a quote outlining the total number of hours required to complete this work, and the total charges for this additional consultancy services using the fixed rate per hour as per the Call-Off Contract. The hourly Consultancy rate under the quote for consultancy work provided by the Supplier will not exceed the Consultancy hourly rates agreed under this Call-Off Contract. The Buyer will review this quote

	and agree any necessary work with the Supplier. Only once the Buyer has provided confirmation to undertake this consultancy work to the Supplier by written notification (an email is accepted as 'written notice') may this consultancy work be completed by the Supplier." [REDACTED]

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: See Onboarding and Offboarding at Part A of this Order Form.
Guarantee	Not applicable.
Warranties, representations	As found in the Supplier Terms, replicated here for ease of reference: We warrant that We are not aware that the Access Product(s) any Documentation, information, data, computer facilities or material that We supply, or Your use of the same in accordance with the terms of this Agreement will infringe any third party's Intellectual Property Rights but We have not carried out any investigation into the same. We shall indemnify You against all direct costs, claims, demands expenses (including reasonable legal costs) and liabilities of whatever nature incurred by or awarded against You arising out of or in connection with any breach of the warranty contained in this clause. We warrant that during the Warranty Period the SaaS, when used in accordance with the Documentation, will operate in all
	material respects in accordance with the Documentation and Specification (where applicable)
Supplemental requirements in addition to the Call-Off terms	Not applicable.

Alternative clauses	Not applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not applicable.
Public Services Network (PSN)	Not applicable.
Personal Data and Data Subjects	Details on how the Supplier processes personal data under this Call-Off Contract is detailed at Schedule 7.

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	Access UK Limited (the Supplier)	Buyer
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Schedule 1: Services

In addition to the Services described at Part A of the Order Form, the Supplier shall provide to the Buyer ongoing support services throughout the term, described as a customer success plan. The customer success plan relevant to the Services procured hereunder is detailed in Schedule 1 of this Order Form

During this Call-Off Contract, the Buyer may identify a requirement for use of MicroVM services, to improve the speed of the system and the accuracy of the data produced. This MicroVM would be to run the heavy routines that produce the Payroll Export File requiring the following steps:

1. building the data. This would be completed by the Supplier's technical developers for the Buyer
2. the 'Checks for Changes' process. This will be tested by the Buyer's Users (HMCTS Bristol team) upon implementation in the live environment. This testing process will proceed in line with the Assurance process agreed between the Buyer and the Supplier in Schedule 1 of this Call-Off Contract document.

If the Buyer identifies the requirement for this MicroVM service from the Supplier, as per the reasons specified above, the Buyer will make the Supplier aware of this additional requirement. The Supplier will then share a specific quote for this MicroVM service with the Buyer. The Buyer will review this quote, and agree any necessary work with the Supplier. Only once Buyer approval in the form of written notification has been received for this quoted specific work (an email is specified as in writing), in line with the Assurance process agreed between the Buyer and the Supplier in Schedule 1 of this Call-Off Contract document, may this work be undertaken by the Supplier.

Completion of development on bulk upload of data to Access

Req No.	Requirement
1	Bulk Upload of fee data from MARTHA, OPT and Crystal data to Access UK Ltd.
2	Bulk input training hours for multiple JOHs to simplify the input procedure.
3	Bulk upload of spreadsheet data
4	Import sitting data from tribunal / court case management systems for validation of JOH claims.

Reconciliation and running of payroll

Req No.	Requirement
1	Reconcile payroll data with the fees claimed so that it is clear what claims have been processed and paid.
2	Export of over 30,000 lines.
3	Payroll V2 (including AP File work).
4	Capacity handling / Slowness of system

Assurance and Governance Processes

The below assurance process is to demonstrate the sign-off of all work developed and delivered by the Supplier to the Buyer throughout this Call-Off Contract. All development work delivered by the Supplier to the Buyer during this Call-Off Contract, including under any extension periods, will follow this below process (unless agreed by both Parties in writing during the Call-Off Contract to amend this Assurance and Governance Process):

No.	Activity	Actions Required	To be Completed By	Estimated Delivery Time	Owner
1	HMCTS identify an improvement for the Access Fees and Expenses System	HMCTS Bristol to write and share their requirements with Access UK Ltd Customer Success Manager via email	HMCTS	5 working days	HMCTS Head JPPT
2	Access UK Ltd to review the requirements provided by HMCTS Team	Access UK Ltd are to review the requirements and complete their response in writing (an email is accepted as in writing) to this request. Access UK Ltd's response shall include: • Activities required for completion • Action leads for each activity (HMCTS Operational Leads, MOJ Commercial, Access Developers, Access Customer Relationship Lead, Access Commercial Director, IT/ Cyber Security Leads etc.) • User Support required, from Access UK Ltd and HMCTS Bristol Team if required • Delivery Times for each stage of the delivery • Total Costs for this delivery • A unique reference for purchase order/invoice use.	Access UK Ltd	5-10 working days	Access UK Ltd nominated lead
3	Further discussion between Access UK Ltd and HMCTS	If further discussion of the proposal is required by HMCTS:	HMCTS	5 working days	HMCTS Access Expense Budget Holder and HMCTS Head JPPT

		• Access UK Ltd will be advised in writing (email is acceptable). • A meeting will be arranged within the 5 working day period. • If necessary, HMCTS will revert to Action 1 for response by Access UK Ltd as per action 2 above.			
4	HMCTS Agreement to Proceed	HMCTS will review the proposal from Access UK Ltd and complete their response in writing (an email is accepted as in writing) to the proposal. The response shall include: • Confirmation of authority to proceed • Confirmation of purchase order/invoicing procedure.	HMCTS	5 working days	HMCTS Access Expense Budget Holder
5	Invoicing procedure begins	• Access Group construct and Max Barrow signs off invoice, corresponding with charges agreed as per step 4. Access send invoice to Nick Randle for HMCTS to approve. • HMCTS confirm receipt, acceptance and sign off of invoice for payment to Access group.	Access UK Ltd/ HMCTS	3 working days	HMCTS Access Expense Budget Holder
6	Management and monitoring of progress of work.	To be reviewed at fortnightly Access UK Ltd/HMCTS JPPT catch ups. • Where re-assessment is needed revert to action 1 above.	HMCTS/Access UK Ltd	Fortnightly	HMCTS/Access UK Ltd

The Service Definitions applicable to the Services to be provided can be found here:

(Access Expense) https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/579935/398860926793187-service-definition-document-2020-04-29-1105.pdf

User Story	Actions to Complete Requirement	Date for Completion
Input of Fees Claims		
As a Claims Processing Officer I want to input a JOHs NI number and have their details displayed so that I can pay their fees	With Development team, no confirmed release date.	
As a claims processing officer I want to be able to bulk input training hours for multiple JOHs so that it simplifies the input procedure.	This needs to be clarified by Buyer. Is this new project?	

As a JOH I want to be able to log on to a web based application so that I can submit my claim electronically	If there are any future cases these will be handled on a case by case basis.	
As a Welsh JOH I would like to see all my input screens in either English or Welsh.		
As a Team Leader / Deputy Team Leader I want to be able to import HR data from the judicial HR system on a regular basis so that JOH data on the system is up to date	If there are any future cases these will be handled on a case by case basis.	
As a Team Leader / Deputy Team Leader I want to be able to reconcile the payroll data with the fees claimed so that it is clear what claims have been processed.		
As a claims Processing Officer I would like any claims for additional fees to be authorised by a designated officer/ regional judge so that only authorised claims are paid.		
Calculation of Fees Due		
As a Claims Processing Officer I want to import sitting data from tribunal / court case management systems so that I can validate the JOHs claims		
Claims Processing Officer - system to highlight if a fee requires approval from a senior judge so that approval is sought before the claim is paid.		
As a Claims Processing Officer I would like the system to highlight any late claims so that they can be handled correctly		
Input of Expenses (Fees and Shared)		
As a JOH I would like the system to check any claim for expenses against existing fee claims records so that they are paid correctly.		
Pensions Reporting (Fee Paid Judges Only)		
Team Leader / Deputy Team Leader I want to be able to produce a pensions data listing so that I can supply the pensions provider with the correct data	This report to be updated once items on bulk upload are completed.	
Input of Sick Pay (Fee Paid Judges Only)		
Claims Processing Officer - have the system check that the JOH was due to sit on a day that they have claimed as sick so that I can pay them correctly		
Reporting		
Team Leader / Deputy Team Leader - run a report that will analyse sitting data venues for office-holders that do not have PHC to identify and pay the London Weighting as a lump sum at the		

end of the year so that these JOHs have their London Weighting paid correctly.		
As a Team Leader / Deputy Team Leader I want to be able to report on the total amount per paid claim so that I can provide management information		
As a Team Leader / Deputy Team Leader I want to be able to create custom reports on the held data so that I can provide management information		
Team Leader / Deputy Team Leader - produce a pay advice for certain tribunals / courts so that JOHs can see what claims have been paid		
Team Leader / Deputy Team Leader - produce a report detailing training payments within a date range so that we can monitor training		
Team Leader / Deputy Team Leader - produce a report detailing all travel within a date range so that we can monitor travel payments		
Team Leader / Deputy Team Leader - produce a report detailing monthly fee/expense amounts so that we can monitor judicial spend		
Team Leader / Deputy Team Leader - produce a report detailing number of sittings so that we can monitor the number of sittings.		
Team Leader /Deputy Team Leader - produce a report detailing the amount of each activity (Training, writing up, etc.) so that we can monitor cost by activity.		
As a Team Leader / Deputy Team Leader I want to be able to produce a report detailing all claims where the tribunal / court is located in Scotland so that we can monitor Scottish tribunal claims.		
As an approved HMCTS/MoJ stakeholder I would like access to the reporting module of the system so that I can produce my own reports.		

Non-Functional Requirements

These non-functional requirements, as provided under previous Call-Off Contracts, have been included and updated for this Call-Off Contract requirements. These requirements must be monitored and continuously delivered by the Supplier to the Buyer throughout the duration of this Call-Off Contract, and under any extension periods to this Call-Off Contract term:

Req. ID	High Level Business Requirement	Requirement for Call-Off Contract period
Audit		

AUD001	All transactions will be recorded in an audit log accessible only to limited users.	All transactions are recorded in an audit log, and can be accessed whenever. Transactions are not removed.
AUD002	The Solution must support audit and accounting and make it possible to match activity to a specific host.	All claims are given a unique reference number which can be reported on.
AUD003	The Supplier must ensure that any electronic transfer of MoJ data prevents repudiation of receipt through accounting and auditing.	The Supplier is to supply Cryptographic standards policy and confirmation of Cypher Suite version used to the Buyer within 30 days of Call-Off Contract signature.
AUD004	The Authority should be permitted security audit rights to the Supplier in order to monitor and review their delivery on security aspects of the Solution where necessary.	
AUD005	The Supplier must ensure that, within legal constraints, audit logs shall be retained for a minimum of six months.	
AUD006	The Solution must have a consistent time source and be synchronised across all accessing devices.	The application woks with a single time source across all platforms.
AUD007	The Authority Must be permitted security audit rights to any Supplier Subcontractors in limited circumstances (specified as a result of the Accreditation process). Monitoring and review of Subcontractor compliance with their delivery on security aspects of the Solution is the primary responsibility of the Supplier.	ISO27001 accreditation provided separately.
Access		
ACS001	The Solution must use a multi factor authentication that is appropriate to the sensitivity of the information it is protecting.	Office 365 Multi Factor Authentication
ACS002	The Solution must provide user identification and authentication controls that prevent entities from accessing other user sessions through cross-contamination.	Using MFA this is negated.
ACS003	The Infrastructure must securely separate consumer data and services from other consumers of the service.	Information provided separately in Access Expense factsheet.
ACS004	The Solution must segregate duties of privileged users to ensure separation of request, approval and processing stages for user/system account: a) creation; b)changes to permissions and policies c) deletion; and d)Access to and processing of protective monitoring logs	Provided in Acceptable Use Policy
ACS005	The Solution privilege management controls must validate user credentials against a directory service for every user action to prevent execution of unauthorised actions.	
ACS006	The Supplier must ensure that all administration access to Solution components is authenticated and accountable to an individual.	
ACS007	The Supplier must ensure that the system provides access controls to prevent unauthenticated users from accessing administrative functions.	

ACS008	The Solution identification and authentication controls for external user connections should require multiple authentication factors prior to granting access in order to prevent unauthorised entities gaining access to services and information.	
ACS009	The Solution must provide user identification and authentication controls that prevent authorised users from creating unauthorised sessions.	
ACS010	The Supplier must ensure that the System provides access controls that deny by default unauthenticated users.	
ACS011	The Supplier must ensure that the System provide directory service controls that match the external identity of a user with an internal account.	Not applicable
ACS012	The Supplier should ensure that the System provides access controls that allow termination of any user session by an administrator or system process to be agreed with the Authority.	
ACS013	The Supplier must ensure that the System provides access controls that, upon user logout, terminate all associated sessions.	
ACS014	The Supplier must ensure that the System provides access controls that automatically terminates user sessions, irrespective of the network activity, after a time period to be agreed with the Accreditor.	1 hour
ACS015	The Supplier must ensure that the System provides user access controls using a directory service that stores and organises access permissions and user attributes.	
ACS016	The Solution must control user access to information using a Role Based Access Control (RBAC) security model	
ACS017	The Supplier must ensure that super user access to the Solution by their administrators can only be performed from within the UK.	
ACS018	The Supplier must ensure that logical access to Solution components by Supplier and support staff is only permitted from secure areas (premises within scope of Provider security policy and ISO27002 controls) and never from a home location.	Provided in Acceptable Use Policy
ACS019	The Supplier could ensure that the system provides connection time limiting controls to prevent users from accessing information and services at hours when the system is not required for the specific activity.	No restrictions on access; solution is available 24x7.
ACS020	The Supplier must provide screening controls that conform to the Baseline Personnel Security Standard (BPSS) for all staff and Subcontractors that have logical or physical access to the Solution or Authority data. Personnel that do not have access must also be cleared to this standard or the Supplier must provide evidence that they have controls to prevent these personnel from gaining access.	Provided in Acceptable Use Policy

ACS021	The Supplier should provide Security Check National Security Vetting for all staff and Subcontractors that have administrative access to the Solution or physical access to Solution support utilities.	
ACS022	The Supplier should ensure that their Solution ICT System Manager and administrators who have Solution 'super user' privileges are UK Nationals.	
ACS023	The Supplier must ensure that all staff and subcontractors users and relevant employees are provided with appropriate security education, training and awareness, with this aspect being reviewed at least annually and whenever personnel roles change. Training shall include elements of physical, personnel and electronic security guidance as well as data handling guidance.	
ACS024	The Supplier must strictly limit access to system source code, related design specifications and configuration data for the Solution to the minimum staff or contractors who require access.	The Supplier is to provide evidence of assurance in meeting the attached requirement to the Buyer within 30 days of the Call-Off Contract Start Date.
ACS025	The Supplier must strictly limit access to backup and log files for the Solution to the minimum staff or contractors who require access.	
ACS026	The Solution must provide a secure means of administering cloud infrastructure services.	The Supplier is provide evidence of assurance in meeting the attached requirement to the Buyer within 30 days of the Call-Off Contract Start Date.
Accreditation		
ACR001	Where virtualisation technologies are used to separate security domains, it must be done in line with GPG 12 - Use of Virtualisation Products for Data Separation.	In Access Expense Factsheet
ACR002	The Supplier must ensure that all data centres which store Authority data are certified to a level agreed with the accreditor.	
ACR003	The Supplier must provide evidence that they have achieved 'Cyber Security Essentials'.	Cyber Essentials Certificate attached
ACR004	The Supplier should develop, maintain and agree with the Authority a Security Management Plan, structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, to cover IA aspects of Solution delivery, support and retirement/migration. The plan should also indicate the accreditation relevant aspects of the Solution.	ISO27001 information provided separately.
ACR005	The Supplier could organise and maintain a Security Working Group initially composed of the Authority's Accreditor and the Supplier's Project Manager, Security Manager and IA adviser as a minimum, who meet on a regular basis as agreed with the Accreditor, to coordinate information assurance and security activities for both the implementation of and the operational life of the Solution.	As per this requirement, the Supplier needs to work with the Buyer to satisfy any IA concerns then commit to monthly meetings focused on security posture.

ACR006	The Supplier should deliver successful Accreditation for the Solution, at no additional cost to the Authority, prior to System "go-live", and maintain the RMADS and Accreditation for the life of the contract. Successful Accreditation is as defined by the Authority Accreditation Framework, in line with the Authority risk appetite, arbitrated by CESG.	
ACR007	The Supplier should use a Requirements Compliance Matrix to demonstrate the level compliance of the Solution	Hasn't been raised by the team. Can be reviewed going forward.
ACR008	The Solution must define and document a cryptographic policy if cryptography is used as a control. This must be in line with industry good practice.	Access maintains cryptographic policies and controls with Salted and Hashed password encryption.
ACR009	The Supplier must ensure that the system provides controls to securely manage (store and propagate) all cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Authority's Cryptographic Policy.	The Supplier is to supply Cryptographic standards policy and confirmation of Cypher Suite version used to the Buyer within 30 days of Call-Off Contract signature.
ACR010	The Supplier must support the Authority's compliance with the Security Policy Framework (SPF).	
ACR011	The Supplier should demonstrate that the technical and non-technical security controls documented within a relevant RMADS are implemented and operating as agreed with the Accreditor by means of compliance audits when requested by the Authority at any time.	Not aware that this has been requested by the Buyer.
ACR012	The Solution must be subject to an independent initial (prior to 'data load for go-live') and regular (in line with the accreditation requirement) penetration test, conducted in line with the accreditation penetration test scope (statement of work).	The Supplier is to supply reports from an ITHC/Penetration test completed within the last 12 months and the follow-on remediation report/s to the Buyer within 30 days of Call-Off Contract Start Date. The Supplier acknowledges that any failure to provide this information to the Buyer within the Call-Off Contract Start Date will result in an independent ITHC performed by HMCTS Cyber Security team on behalf of the Buyer.
ACR013	The Supplier must ensure that the system uses products that are certified under the relevant CESG Assurance Scheme to the appropriate grade, for any security enforcing functionality within the Solution, including connections to the PSN which must be CPA Foundation grade.	We are G Cloud certified so that is covered by this. See '14 principles of Cyber security' attached.
ACR014	The Supplier must ensure that all identified residual risks are treated to the satisfaction of the Authority with residual risks accepted prior to 'go-live'.	The Supplier is to supply reports from an ITHC/Penetration test completed within the last 12 months and the follow-on remediation report/s to the Buyer within 30 days of Call-Off Contract Start Date. The Supplier acknowledges that any failure to provide this information to the Buyer within the Call-Off Contract Start Date will result in an independent ITHC performed by HMCTS Cyber Security team on behalf of the Buyer.
ACR015	The Supplier should evidence the implementation of ICT Service Management Considerations in line with GPG20	

ACR016	The Supplier must have Acceptable Use Policies that have been agreed with the Authority in place. The policy must include but not be limited to statements reminding users to only use the Solution for authorised purposes. Users must positively confirm their acceptance of the policy. An electronic receipt must be issued and stored for the purpose of auditing.	
ACR017	The Supplier shall consider the PSN Incident Management process in developing and implementing incident response processes.	The Supplier is to provide incident management policy and BCP/DR Policies to the Buyer within 30 days of Call-Off Contract Start Date.
ACR018	Should removable media be required, the Supplier must have a policy for removable media that addresses the risks of using removable media. This must form a part of an overall risk management approach	
ACR019	The Supplier will provide any information required to assess the security assurance position of the solution to achieve accreditation.	The Supplier agrees to provide information and evidence required to achieve accreditation to the Buyer within 30 days of Call-Off Contract Start Date.
ACR020	The supplier should deliver the service under a certified ISO/IEC27001 ISMS	
ACR021	The Supplier should engage an independent penetration testing company that is part of the CHECK scheme to conduct an ITHC on the solution.	The Supplier is to supply reports from an ITHC/Penetration test completed within the last 12 months and the follow-on remediation report/s to the Buyer within 30 days of Call-Off Contract Start Date. The Supplier acknowledges that any failure to provide this information to the Buyer within the Call-Off Contract Start Date will result in an independent ITHC performed by HMCTS Cyber Security team on behalf of the Buyer.
ACR022	The Solution should allow End Users to manage their passwords securely. As part of this management, the Solution should offer a configurable password history length and configurable password complexity rules that are in line with the MoJ Password Policy	
ACR023	The Solution should ensure user accounts where the terms and conditions of service have not been accepted are disabled.	No change. There is no terms and conditions which a user has to tick in order to gain access to the application.
ACR024	The Supplier must define, document and agree with the Authority the roles and responsibilities of their staff and Subcontractors whom are responsible for delivering, administering and operating the Solution.	The administrators have been defined by the Buyer to have the relevant access to the application.
ACR025	The Supplier should develop and maintain an accurate inventory of the information, system, hardware and software assets used to deliver the System and Service.	Access to supply the relevant inventory and the wider CMBD (Config management Database) to the Buyer within 30 days of Call-Off Contract Start Date.
ACR026	The Supplier must define and inform the Authority of their incident point of contact with their contact information.	

ACR027	The Supplier must evidence to the Authority its internal incident response processes for identifying and responding to security incidences. The evidence must include a process for involving the relevant and nominated security incident response companies	The Supplier is to provide incident management policy and BCP/DR Policies to the Buyer within 30 days of Call-Off Contract Start Date.
ACR028	The Supplier must have in place a configuration control process which prevents unauthorised changes to the standard build of network devices and hosts. This process must be compliant with relevant Authority policies	See change management policy
ACR029	If Active Content is required the code must be subject to security review, configuration control and digitally signed. The system must ensure that no unsigned Active Code is capable of being executed on the System.	The Supplier is to supply reports from an ITHC/Penetration test completed within the last 12 months and the follow-on remediation report/s to the Buyer within 30 days of Call-Off Contract Start Date. The Supplier acknowledges that any failure to provide this information to the Buyer within the Call-Off Contract Start Date will result in an independent ITHC performed by HMCTS Cyber Security team on behalf of the Buyer. It is digitally signed.
ACR030	If Active Content is required, the Solution shall implement controls to ensure that executable content shall not be run without the user's active consent' and within the organisation's control	
ACR031	The Solution should notify users to read and accept the terms and conditions of service annually in line with the acceptable use policy.	Not implemented.
ACR032	The Supplier must develop, maintain and agree standard configuration builds for all Solution platforms. All builds must only have services, functionality and features enabled that are essential for meeting the Authority's requirements.	
ACR033	The Supplier should ensure and demonstrate that the system code is developed according to industry and government best practice and standards, in a format to be agreed with the Accreditor.	
ACR034	The Solution security-related controls should be designed, developed, tested and implemented within the UK and by UK nationals.	.
ACR035	The Supplier must ensure that any subcontracted suppliers follow the System Security Aspects Letter	
ACR036	The Supplier should ensure that any subcontractors meet Cyber Security Essentials or are certified to ISO27001	
Accessibility		
ACC001	The application should comply with the Disability Discrimination Act	We do not comply to this.
ACC002	The application should follow industry and government best practices for accessibility. The cross government minimum standard is WCAG 1.0 AA	

ACC003	The solution must be fully compatible with commonly used Assistive Technology tools, such as: - Ai Squared Zoom Text Magnifier screen magnification software - Nuance Dragon Naturally Speaking speech recognition software - TextHelp Read and Write reading and writing support software - Dolphin SuperNova screen magnification, speech and Braille output software	
ACC004	The system and its records shall be compliant with the Welsh Language Act.	
Availability		
AVA001	The system must be available 24 hours a day	
AVA002	A helpdesk facility must be available between the hours of 08:00 and 18:00 Monday to Friday	
AVA003	Planned maintenance must be scheduled during the weekend or when demand on the system is low	Any planned maintenance is done on times which causes as minimal interruption as possible.
AVA004	The business can cope with the loss of availability of the Solution following a non-catastrophic unplanned outage for a maximum duration of 24 hours	Data is replicated across 2 datacentres. BCP provided separately.
AVA005	The business can cope with the loss of availability of the Solution following a catastrophic unplanned outage for a maximum duration of 48 hours	
AVA006	Toleration of Data Loss in the event of recovery following any outage = 5%	
Archive		
ARC001	The application must hold data only for as long as is specified by the data retention schedule for the pertaining business unit (Currently 6 years)	No parameters have been set. Data is currenlty retained for as long as you require.
ARC002	Data that is required but rarely accessed could be archived to an offline data store	We can export data to an offline source is required. We just need to know volumes of data, and can then provide more information on processes.
ARC003	The application should have the ability to restore data that has been archived to the offline store on user request	
ARC004	The restoration of data should take no longer than 1 working day from the point of the request being made	This is dependent on the volume and source of the data.
Data Integrity		
DAT001	The Supplier must ensure that any electronic transfer of MoJ data maintains the Integrity of the data during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data.	Resilience testing is generally applied to applications that operate under stress / chaotic conditions. This is SaaS software that relies on the infrastructure that houses is and Access uses multiple technologies for capacity management , disk usage and the environment is constantly monitored by the Operations team through Rapid 7 SIEM

DAT002	The Solution must provide data back-up controls that conform to the data back-up policy to prevent data from being permanently lost or corrupted following accidental or deliberate storage failures.	
DAT003	The Solution must provide input data validation controls to validate all data that is received from external system sources.	External data needs to be validated before it can be accepted into the system. Essentially it ensures the fields to be imported meet the necessary criteria.
DAT004	The Solution should provide internal processing controls that assure the integrity of communications between architecture tiers to prevent malicious data in higher tiers exploiting vulnerabilities in lower tiers.	Correct, covered in separate documentation.
DAT005	The Solution should provide internal processing controls between architecture tiers to detect data corrupted in transit.	
DAT006	The Solution should provide output validation controls to prevent data being corrupted in transit.	
Data Protection		
DAP001	The Supplier must ensure that any electronic transfer of MoJ data protects the Confidentiality of the data during transfer through encryption suitable for the impact level of the data.	
DAP002	The Solution must have a data back-up policy that defines the types of data to be backed-up and how and when they must be backed-up. The policy must also define the data retention requirements for the data being backed-up if applicable, as specified within the data retention policy.	Yes, restore tests ae carried out on backups.
DAP003	The Supplier must ensure that the System provides cryptographic controls that protect the confidentiality of data at rest on media devices.	Yes
DAP004	The Supplier must ensure that all data relating to the system as claimants is stored within the UK.	
DAP005	Data that is to be removed from the system should not be recoverable and the method of sanitisation used should be tested to provide assurance of its effectiveness.	
DAP006	Equipment used to deliver the service that is no longer required should be disposed of in line with ISO27001 or an appropriate standard as agreed with the Authority.	
DAP007	The Solution must have a data retention policy that specifies for all types of data processed how long they must be retained and the method in which they must be disposed when the retention period has expired.	
DAP008	The Supplier must ensure that the system provides storage controls to ensure that data within the Solution components is only retained for the required retention period as defined by the data retention policy.	

DAP009	The Supplier should provide information to allow the Project to ensure that the system provides controls that manage any privacy impacts identified within the privacy impact assessment, to be completed by the Authority.	Access are GDPR compliant, information on this provided separately.
DAP010	The Supplier must comply at all times with the Data Protection Act 2018 and shall not perform its obligations under the Contract in such a way as to cause the Authority to breach any of its applicable obligations under the Data Protection Legislation.	
DAP011	The Supplier must ensure that none of the Supplier's staff or contractors publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority.	
DAP012	The Supplier must process the Personal Data, for lawful purposes, only to the extent, and in such manner, as is necessary for the provision of the MoJ Services.	
DAP013	The Supplier should ensure all staff and contractors who may have the capability to view data held within the Solution have signed personnel Confidentiality Agreements or Non-Disclosure Agreements whenever their role or privileges provide the capability to view Authority's data/information or the system.	
Design		
DES001	The solution will not require the installation of an executable on the desktop i.e. the solution will be 'thin client'.	
DES002	The solution will not require the use of browser plug-ins.	
DES003	The solution design will utilise open source products wherever possible	
DES004	The solution will be platform independent	Access Expense is platform independent. Other applications can be used within Workspace, but these are separate.
DES005	It will be possible to obtain time from a reliable Authority approved time source, synchronising all elements of the solution to that source. The solution will include regular reviews of synchronisation across the solution.	
DES006	The clock will be able to cater for changes in time from B.S.T to G.M.T and vice versa without disruption to the service.	
DES007	The solution will be capable of handling at least all dates between 1900 and 2100, including all date/time changes.	
DES008	It will be possible to "copy and paste" data between templates within the Application, and between the Application and other Applications.	
DES009	The system will present the majority of input as drop down menus or option buttons	
DES010	The system will have some form of online help facility	

DES011	The vendor will provide a user helpline	
DES012	The vendor helpline will be active between the times of 07:00 to 19:00 Monday to Friday	
DES013	Each web page will contain the appropriate branding (logos, corporate style, etc.)	
DES014	The system produces error messages, which are meaningful and appropriate, and offers immediate prompts for actions to resolve the error wherever possible.	
Maintenance		
MAI001	The solution will be one that the vendor is actively developing and supporting (i.e. not near the end of its product life)have a minimum support life of 10 years	Quarterly.
MAI002	Whoever supports the system must give at least 48 hours' notice of any downtime necessary for system maintenance	We try to give as much notice as possible for any downtime and will adhere to 48hrs as a minimum. The latest update gave 14 days' notice.
MAI003	The Solution must not have authentication lock-outs on service accounts.	
MAI004	The Solution should be managed through a physically separated management network, using dedicated management ports, consoles and terminals to prevent any unauthorised internal or external entity accessing	We use VLAN.
MAI005	The Supplier must ensure that appropriate controls are in place to prevent malware ingress through removable media connecting to any Solution infrastructure hardware or any Supplier systems used for development,	
MAI006	The Supplier must ensure that remote Solution management is not performed from/over untrusted networks.	
MAI007	The Service management model should be validated through a recognised audit scheme (e.g. ISO27001/CSA CCM v3.0).	We abide by ISO27001. More information provided separately.
MAI008	The Supplier must ensure that all components (including but not limited to software, hardware and firmware) of the Solution are patched in line with the Authority's Patching policy; the approach to this must be documented	The Supplier is to provide Patching policy and identify key timelines used for system upgrade in the forthcoming calendar year, to the Buyer within 30 days of the Contract Start date.
MAI009	The Supplier must ensure that patches shall be applied with minimal delay and audited to ensure compliance with the organisation's policy, in line with the MoJ Patch Management Standard.	The Supplier is to provide a patching history enabled and to provide any significant change control logs used for services to the Buyer within 30 days of the Contract Start date.

MAI010	The Supplier should commit to resolving all technical vulnerabilities, identified from vendor releases, penetration tests and vulnerability scans on the Solution. Options for resolution include but are not limited to: • use of appropriate security features • changes to system architecture • application of relevant patches • avoided i.e. components turned off; or • any associated risk accepted, • in line with the accreditation requirement	
Back up		
BAC001	A Disaster Recovery strategy shall be required for the system.	We do not share test results, but anything found is fixed immediately. Last test Dec 2020.
BAC002	Fully documented disaster recovery processes and plans for the service will be in place before the service goes live. The Contractor shall store these plans in the Document Repository and a copy sent to ITSCM team.	The Supplier is to provide their disaster recovery processes and plans to the Buyer within 30 days of the Contract Start date.
BAC003	Automated backup, archive, and retrieval processes must be in place, including documentation, prior to go live	
BAC004	Automated backup / recovery procedures must take into account system growth and specify such things as what is to be backed up, size, type of backup and ensure compatibility with existing infrastructure.	
BAC005	All key software, configuration settings, databases, flatfiles and state data will be backed up should there be a need to reload or restore them	
BAC006	Backups must fit in with the existing backup schedule	The Supplier to verify if back-ups been tested in IT Health check planning and provide this information to the Buyer within 30 days of the Call-Off Contract Start Date.
BAC007	The system will be backed up to secure media at least once every 24 hours	
BAC008	The restoration of data from a secure backup will be tested regularly	Supplier to provide reporting log to the Buyer within 30 days of the Call-Off Contract Start Date.
BAC009	Capability should exist to restore only the data item that is required. E.g. An entire database should not have to be restored to recover a single file	
Interfaces		
INF001	The Supplier should provide information to the Project to support the Project producing a data exchange agreement for every type of data transfer with another system, including MoJ and any Authority system. This agreement should be approved by Authority's Information Asset Owner of the data and detail: • What information can be exchanged? • What is the mechanism for exchange?	There are different integrations setup. Please clarify.

	• How should the information exchanged be handled by both parties? • How will the exchange be secured? • Who authorises the exchange? • How long is the agreement in place for?Who is responsible for managing the security of the exchange?	
INF002	The Solution must provide network segregation controls that prevent external entities and services from gaining direct access (or sending direct requests) to internal resources.	
INF003	The Solution must provide network connection controls that prevent unauthorised entities from connecting to external facing services.	
INF004	The Supplier must ensure that the system provides network controls that limit the externally-available network services to only those necessary for external Solution users.	
INF005	The Solution must provide network routing controls at the perimeter that prevent unauthorised communications between external and internal resources.	
INF006	The Supplier must ensure that the system provides network routing controls and physical network architecture that prevents network traffic from bypassing other network access controls.	
INF007	The Supplier must ensure that the system provides network routing controls at the perimeter that prevent unauthorised external parties from accessing the internal system.	
INF008	The Solution must provide network routing controls to prevent internal resources communicating with unauthorised entities and services.	
INF009	The Solution's external interfaces must be CHECK tested to ensure they are both robust and necessary for the operation of the service.	
INF010	The Supplier should provide infrastructure connectivity between the Solution and the Authority's protective monitoring provider's system.	
INF011	The Supplier must ensure that services traversing gateways/boundary controls shall be minimised to those required to carry out the business function	
Interoperability		
INT001	Interfaces with internal and external parties will comply with HMG standards	
Scalability		
SCA001	The supplier should be able demonstrate that application is inherently ‘scalable’. Greater computational resource should be able to be added and utilised by the application to provide a commensurate return in performance and capacity	Access monitors servers to ensure sure they are available as well as having thresholds in place to alert us of capacity issues. Alerts are generated if there is a "near" capacity issue and we run the hardware environment at N+1. Repeat alerts would generate a review on a server and there is constant monitoring through management review and operational meetings
Logging		

LOG001	The Supplier must ensure that the system provides controls that log and collect events, as specified within the MoJ protective monitoring policy, into localised storage areas to support the detection of malicious activity.	
LOG002	The Supplier must ensure that all Solution components are capable of being interrogated by third-party log agents to retrieve locally-stored log data, to ensure compatibility with the external protective monitoring provider.	This forms part of the PEN testing
LOG003	The Supplier should provide ongoing security management, including Authority reporting and remedial action, of relevant output from the protective monitoring provider, as agreed with the Accreditor.	
LOG004	The Supplier should review their administrator and operator Solution logs for malicious activity in line with the protective monitoring policy.	
LOG005	The Solution must support the logging of failed access attempts through log in mechanisms such as single sign-on.	
LOG006	The Supplier should ensure that the System provides management controls that display user session history to authenticated administrators.	
LOG007	The Solution must record all the actions in line with the Security Policy Framework, the MoJ Protective Monitoring Policy, and guidance from GPG13 (including but not limited to view, create, delete, update) of Administrative	
LOG008	The Solution must record the appropriate actions (in line with the Security Policy Framework, the MoJ Protective Monitoring Policy, and guidance from GPG13, and as agreed with the Authority) of all authenticated End Users.	
Legal		
LEG001	The Solution and Service Provider[s] shall process all personal data in accordance with the Data Protection Act 2018.	
LEG002	The system and its records shall be compliant with the Gender Recognition Act 2004.	
LEG003	The system and its records shall be compliant with the Welsh Language Act.	
Capacity		
CAP001	The system shall allow for records to be deleted when they no longer meet the Data Retention Policy	This would be done by one of the infrastructure team, and only at the written request of the Buyer.
CAP002	The system should have sufficient storage to cope with the predicted data storage requirements for the lifetime of the system or have a plan and budget in place for upgrading	Access have over 1,000,000 users on Workspace with ambitions for that to double in 2 years. We are constantly evaluating and ensuring there is sufficient storage to maintain the applications.
CAP003	The solution must be able to support 360,000 records per year (10% increase included)	As above, there are plans for that to increase manifold to be in line with usage.

CAP004	System will support: 11000 total users (10% increase included)	
CAP005	The system will be capable of processing over 85,000 manual claims per year	Claim volumes are reviewed by the team in quarterly meetings to ensure system can manage with expense volumes.
Security		
SEC001	The Solution must provide data back-up controls that prevent entities from gaining access in transit.	The Supplier is to supply Cryptographic standards policy and confirmation of Cypher Suite version used to the Buyer within 30 days of Call-Off Contract signature.
SEC002	The Solution must provide network controls that prevent unauthorised entities from gaining access to sensitive data in transit outside of the network boundary.	The Supplier is to supply Cryptographic standards policy and confirmation of Cypher Suite version used to the Buyer within 30 days of Call-Off Contract signature.
SEC003	The Solution must only communicate with an authenticated user's device using an appropriately encrypted communication channel.	The Supplier is to supply Cryptographic standards policy and confirmation of Cypher Suite version used to the Buyer within 30 days of Call-Off Contract signature.
SEC004	The Supplier must ensure that physical access to areas that store and process Authority data and assets are controlled and granted on a 'need to know' basis to a minimum staff and contractors required.	
SEC005	The Solution must ensure all passwords are stored in a one-way encrypted file. Where hashing or encryption algorithms are being considered, the supplier must justify any deviations from industry best practice.	
SEC006	The Solution must ensure that all authentication data (including but not limited to usernames, passwords and session data) will be encrypted and/or hashed during transportation and electronic transmission. Where hashing or encryption algorithms are being considered, the supplier must justify any deviations from industry best practice.	The Supplier is to supply Cryptographic standards policy and confirmation of Cypher Suite version used to the Buyer within 30 days of Call-Off Contract signature.
SEC007	The Supplier must ensure that all staff and contractors that have access to the system processing the Authority's data maintain their account passwords in line with the system password policy that must be produced in line with the Authority's Password policy.	
SEC008	The Supplier must enforce the system password policy for all users, including staff and contractors, which must be produced in line with the Authority's policy.	The password policy is the same across all applications. Password policy can be configured by client using Access Identity.
SEC009	The Solution must provide controls to securely manage (create, store and propagate) user credentials to prevent malicious entities and services gaining access to them.	
SEC010	The Supplier must ensure that the system provides each user of the system and its support environment with a unique user ID that they are accountable for, to ensure non-repudiation within the Solution. User IDs must never be shared amongst users.	

SEC011	The Supplier must ensure that the System provides network controls that mutually authenticate internal system components prior to communication	
SEC012	The Solution must remove all information from the screen apart from a login screen, once the configurable session time-out has been triggered.	
SEC013	The Solution must lock-out a user account after five consecutive failed login attempts.	Can be configured by client using Access Identity.
SEC014	The Supplier should ensure that the system provides session time-out controls to suspend or shutdown sessions after a pre-defined period of inactivity to be agreed with the Authority	Times cannot be set by the Buyer, they are fixed.
SEC015	The Solution should notify the user that their session will be suspended or shut down after a pre-defined period of inactivity at initial log-on and prior to suspension/shutdown with the effect this event will have on their session.	
SEC016	The Solution must provide controls that prevent malware from being logically ingressed or physically introduced to services and executed	This is covered in Pen Tests
SEC017	The Solution must provide controls that detect and appropriately correct when malware is logically ingressed or physically introduced to services.	
SEC018	The Solution malware controls must be configured in line with the malware protection guide.	
SEC019	The Solution must provide network controls that detect and appropriately correct intrusion from external entities.	This is not a standard request from consumers, so therefore needs to be provided at a cost.
SEC020	The Solution should provide controls that monitor malicious events and provide appropriate corrective updates and actions, as specified in the incident management plan.	
SEC021	The Supplier must create an incident management plan agreed with the Authority that defines security incidents, response processes and reporting, and corrective actions, as described in the SAL.	The Supplier is to provide the incident management plan (including actions for mitigation) and log of any incidents which may have been recorded over the past periods with any remediation logs to the Buyer within 30 days of the Call-Off Contract Start Date.
SEC022	The Supplier must respond to and report incidents as defined and specified within the incident management plan.	
SEC023	The Supplier must report Solution security vulnerabilities as specified within the incident management plan.	Access do not reveal details of incidents.
SEC024	The Supplier must ensure that the system provides controls that prevent unauthorised access and modification to protective monitoring tools and their communications.	
SEC025	The Supplier should ensure that the System provides network connection controls that prevent denial of service attacks from external sources.	
SEC026	The Supplier should ensure that all data traversing to and from the System's services/networks shall be subject to content analysis including virus checking emails and attachments at the PSN-gateway and host.	

SEC027	The Supplier shall filter against a white list of allowed attachment file types. The white list will be owned and managed by the Supplier and be included as part of the organisation's overall risk management approach.	There are no restrictions on file types to be uploaded.
SEC028	The Supplier should ensure that firewall and gateway servers shall carry out security services to identify malware and vulnerability exploiting code at the gateway. Where encryption prevents this the organisation shall implement an equivalent level of protection at the end point.	
SEC029	The Solution should implement protective monitoring aligned to the Security Policy Framework, the MoJ Protective Monitoring Policy, and guidance from GPG13. Any deviations from guidance should be justified.	
SEC030	The Supplier must define, document, agree with the MoJ, and regularly maintain (at least annually) System Security Operating Procedures (SyOPs) for system administration and maintenance of the Solution, in line with the support and Accreditation requirements, setting out the procedural measures that function as protective controls for each user role.	This forms part of the CSM reviews that take place quarterly.
SEC031	The Solution should have all services hardened and minimised to those essential to the business requirement. This should be validated by a security penetration test before live data is loaded.	Forms part of PEN testing.
SEC032	The Supplier should ensure that the System provides assured gateway/boundary controls between the system components and security domains, such as by using CESG Assured Products for boundary controls.	Supplier uses a Cisco firewall.
SEC033	The Solution must provide input data validation controls to prevent malicious data from exploiting service vulnerabilities and from being inputted incorrectly.	Forms part of PEN testing.
SEC034	The Solution should provide internal processing controls between architecture tiers to prevent malicious data in higher tiers exploiting vulnerabilities in lower tiers.	Forms part of PEN testing.
SEC035	The Solution should provide internal processing controls between security domains to prevent a low domain from exploiting vulnerabilities in a high domain.	
SEC036	The Solution must provide output validation controls to prevent unauthorised data from being exported to unauthorised external entities and services.	
SEC037	The Supplier must ensure that the system code is subject to a security assessment against common issues to the satisfaction of the Accreditor, including the OWASP Top Ten Application Security Vulnerabilities.	

SEC038	The Solution must have information leakage controls to prevent accidental export of internal data through legitimate communication channel feedback.	
Testing		
TES001	The application supplier must produce a Supplier Test Policy document which describes how the supplier's test regime will comply with the MoJ PPD Test Strategy.	
TES002	The application supplier must produce a Project Test Strategy document setting out the strategy for testing for the project in accordance with the Supplier Test Policy and project	
TES003	The system shall be developed using secure programming practices	
TES004	No changes will be performed on the production service unless adequately tested	The Supplier to provide the Buyer with the testing Log of where all tests processes have been approved and committed to service within 30 days after the Call-Off Contract Start Date.
TES005	The Supplier must ensure that their development and test environments for the Solution are separated from the live system, and do not process real Personal Information.	The Supplier have previously confirmed they do not test in live, and are to provide the Buyer with issue of test logs.
TES006	The Supplier must not use any Authority sensitive, personal or Protectively Marked information as test data. Where unavoidable, the data must be protected according to its Protective Marking after seeking Accreditor approval.	We use an anonymised dataset, which can have two different user types. One to assign right permissions for data anonymisations.
Training		
TRA001	The system vendor will be able to provide staff training	
TRA002	The system vendor will supply sufficient documentation for a user to be able to use every function of the system	
TRA003	Any changes to the system in future will be reflected in the training documentation by the supplier.	

Schedule 2: Call-Off Contract charges

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

[REDACTED]

Consultancy services are called off by the Buyer (HMCTS) when required. The Buyer will agree consultancy work to be carried out and will advise the Supplier of required consultancy work. The Supplier will provide the Buyer with a quote outlining the total number of hours required to complete this work, and the total charges for this consultancy work using the fixed rate per hour as per the Call-Off Contract.

The hourly Consultancy rate under the quote for consultancy work provided by the Supplier will not exceed the Consultancy hourly rates agreed under this Call-Off Contract. The Buyer will agree the quoted time and charges for this consultancy work, and notify the Supplier of this agreement, in advance of any quoted consultancy work taking place by written notice. Only once the Buyer has provided confirmation to undertake this consultancy work to the Supplier by written notice (an email is accepted as 'written notice') may this consultancy work be completed by the Supplier.

Where the Buyer has a requirement for any additional consultancy services from the Supplier, the Buyer will make the Supplier aware of these additional consultancy service requirements (as per the Assurance process above). The Supplier will provide the Buyer with a quote outlining the total number of hours required to complete this work, and the total charges for this additional consultancy services using the fixed rate per hour as per the Call-Off Contract.

The hourly Consultancy rate under the quote for consultancy work provided by the Supplier will not exceed the Consultancy hourly rates agreed under this Call-Off Contract. The Buyer will review this quote and agree any necessary work with the Supplier. Only once the Buyer has provided confirmation to undertake this consultancy work to the Supplier by written notification (an email is accepted as 'written notice') may this consultancy work be completed by the Supplier."

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

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).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (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
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.

Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of 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
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.
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.

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any 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.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity
	• reward that person for improper performance of a relevant function or activity
	• commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.

Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

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

Annex 1: Processing Personal Data

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

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

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

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

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

3.3 The Supplier's GDPR Portal is found at: https://access-support.force.com/Support/s/gdpr-hub , to register for access, please email [REDACTED]

1.6 The Product Fact sheets are found within the GDPR Portal. These contain the details of how personal data is processed under the agreement.

Descriptions	Details
Identity of Controller for each Category of Personal Data	The Buyer is the Controller. The Supplier is the Processor.
Duration of the Processing	For the duration of this Call-Off Contract agreement. The final date of processing will be the Call-Off Contract End Date

Nature and purposes of the Processing	As applicable to Dimensions: The Supplier as processor will receive data uploaded to the service by users, which is stored in a cloud environment or on premise in accordance with the options selected by the Buyer (the Controller). The Buyers' users may instruct the service to share some or all of the data with other users or groups/classes of users. As applicable to Expenses: The Supplier as Processor shall receive data uploaded to the service by the Buyers' users, which is stored
	in a cloud environment in accordance with the options selected by the Buyer. The Buyers' users may instruct the service to share some or all of the data with other users or groups/classes of users. As applicable to Insight: The Supplier as Processor shall receive data uploaded to the service by users, which is stored in a cloud environment in accordance with the options selected by the Buyer. The Buyers' users may instruct the service to share some or all of the data with other users or groups/classes of users. The Supplier shall process the Buyers' users User Name, the service, provide support and maintenance services

Type of Personal Data	As applicable to Dimensions for the Buyers' users: forename, middle name(s), surname, title, age, date of birth, nationality, citizenship, occupation, name and locations of places of employments, car registration number, bank details, work email addresses, personal email addresses, work telephone numbers, personal telephone numbers, job title of Fee Paying and Non-Fee Paying Judicial members including Non-Legal Members for Her Majesty's Courts and Tribunals Service. As applicable to Expenses - the data includes but is not limited to the following types of personal data: forename, middle name(s), surname, title, age, date of birth, nationality, citizenship, occupation, name and locations of places of employments, car registration number, bank details, work email addresses, personal email addresses, work telephone numbers, personal telephone numbers, job title of Fee Paying and Non-Fee Paying Judicial members including Non-Legal Members for Her Majesty's Courts and Tribunals Service. As applicable to Insight: Buyers' usernames only
Categories of Data Subject	Fee Paying and Non-Fee Paying Judicial members (including Non-Legal Members) for Her Majesty's Courts and Tribunals Service
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or	a. Data will be returned or deleted (per the Buyer's instruction) within 10 days following the Call-Off Contract End Date. The Buyer's instruction will be provided by the appropriate
Member State law to preserve that type of data	Project Lead for the Buyer in the form of writing, and agreed as part of the exit management plan for this Call-Off Contract."

Annex 2: Joint Controller Agreement

Not applicable.