Crown
Commercial
Service

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

Contents

Part A - Order Form

<table>
<tr><td>Digital Marketplace service ID number:</td><td>231101759078112</td></tr>
<tr><td>Call-Off Contract reference:</td><td>con_17896</td></tr>
<tr><td>Call-Off Contract title:</td><td>Professional Users Access Scheme</td></tr>
<tr><td>Call-Off Contract description:</td><td>Administration and maintenance of security access pass</td></tr>
<tr><td>Start date:</td><td>15th June 2020</td></tr>
<tr><td>Expiry date:</td><td>14th June 2022</td></tr>
<tr><td>Call-Off Contract value:</td><td>
<table>
<tr><th>Year</th><th>Requirement</th><th>Fixed Price cost</th><th>Maximum Contract Value</th></tr>
<tr><td>1</td><td colspan="3" rowspan="4">REDACTED</td></tr>
<tr><td>2</td></tr>
<tr><td>3</td></tr>
<tr><td>4</td></tr>
<tr><td colspan="4">TOTAL MAXIMUM CONTRACT VALUE £1,000,000</td></tr>
</table>
</td></tr>
</table>

Charging method:	The following Charging methods will be available to use under this contract and will be called out in the individual Work Packages: • Fixed Price for implementation and BAU support (the latter will have a range of pricing that maybe changed as the scheme increases in users) • Time & Material (T&M) for any subsequent development work • Other Pricing method or a combination of pricing methods agreed by the Parties
Purchase order number:	TO BE ADVISED

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

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

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

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

From: the Buyer	REDACTED
To: the Supplier	Smart Citizen Ltd 01872 250161 Supplier's address: Unit 3, Building B, Green Court, Truro Business Park Truro Cornwall, TR4 9LF Company number: 4796316
Together: the 'Parties'	

Principle contact details

For the Buyer:	REDACTED

For the Supplier:	REDACTED

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 15h June 2020 and is valid for 24 months.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least [90] Working Days from the date of written notice for undisputed sums or at least [30] days from the date of written notice for Ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for two period(s) of up to twelve months each, by giving the Supplier one month's written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. [The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each. Under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS) if the: ● Buyer is a central government department ● contract Term is intended to exceed 24 months]

Buyer contractual details

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

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud software
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: • Work collaboratively with the HMCTS Project Team planning and implementing the transition from the pilot PUAS system to their system including any required training • Provide and maintain an IT system to support the PUAS • Provide licenses for use of the system • Provide line 2 & 3 IT support to the scheme • Produce the required management information for the relevant governance and contract meeting as specified in the contract. For full details of the service requirements please refer to Schedule 1 for a full list of requirements.

	Please note that the PUAS is expected to have approx. 3000 members and 300 users at scheme go-live this is expected to increase over the contract term. However, HMCTS make no guarantee of service volumes.
Additional Services:	• Undertake any future development work identified
Location:	The Services will be delivered across the HMCTS estate. However, it is not expected that the supplier will need to visit these physical locations and that the majority of the service can be delivered from the Supplier's own offices. For collaboration purposes the base location will principally at the Buyer's offices at although travel to other office may be requested on occasion.
Quality standards:	The quality standards required for this Call-Off Contract are as per Schedule 1 Service Description and to be delivered in conformance with the GDS Service manual. The capability descriptions are to align (where applicable) to Digital, Data and Technology (DDAT) Profession Capability Framework.
Technical standards:	The technical standards required for this Call-Off Contract are as per Schedule 1 Service Description and to be delivered in conformance with the GDS Service manual. The capability descriptions are to align (where applicable) to Digital, Data and Technology (DDAT) Profession Capability Framework.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as per Schedule 1 Service Description.
Onboarding:	The onboarding plan for this Call-Off Contract shall be as per the Supplier's proposed implementation plan which shall be finalised and agreed in writing with HMCTS no later than 2 weeks following signature of this order.
Offboarding:	The offboarding plan for this Call-Off Contract: Off-boarding plan shall be finalised and agreed in writing with HMCTS no later than 2 weeks following signature of this order.
Collaboration agreement:	Maybe required with independent bodies using the scheme – tbc
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed £1,000,000. The annual total liability for Buyer Data defaults will not exceed 125% of the maximum possible capped Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other defaults will not exceed 125% of the maximum possible capped Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance:	The insurance(s) required will be: ● [a minimum insurance period of [6 years] following the expiration or Ending of this Call-Off Contract] ● [professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)] ● [employers' liability insurance with a minimum limit of £5,000,000 or

	any higher minimum limit required by Law]
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit:	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: • clauses 7.4 to 7.13 of the Framework Agreement.
Buyer's responsibilities:	The Buyer is responsible for: • Provision of hardware that scheme users will access the services from • Agreements with Independent Bodies who use the scheme • Provision of Line 1 support and some Line 2 & 3 as defined in Schedule 1 Service Description.
Buyer's equipment:	The Buyer's equipment to be used with this Call-Off Contract includes : as per Buyer's Responsibilities.

Supplier's information

Subcontractors or partners:	The following is a list of the Supplier's Subcontractors or Partners N/A

Call-Off Contract charges and payment

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

Payment method:	The payment method for this Call-Off Contract is BACS.
Payment profile:	The payment profile for this Call-Off Contract is: Tied to milestones delivery for the implementation and then monthly in arrears. Payment profile for any additional work shall be agreed by both parties as part of the change control process.
Invoice details:	The Supplier will issue electronic invoices: • For implementation – once written confirmation has been received that the relevant milestone has been achieved • For BAU services – monthly in arears The Buyer will pay the Supplier within [30] days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to REDACTED Please cc: The Operational Contract Manager as they will need to goods receipt.
Invoice information required – for example purchase order, project reference:	All invoices must include • PO Number, • Contract Reference Number,
Invoice frequency:	Invoice will be sent to the Buyer as above.
Call-Off Contract value:	The total value of this Call-Off Contract is capped at £400,000.00 for the initial term. The value of each extension option shall be capped at £300,000.00 per year.

Call-Off Contract charges:	The breakdown of the Charges is – Please see schedule 2 below

Additional Buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include implementation plan, exit and offboarding plans and milestones.
Guarantee:	Not Required
Warranties, representations:	n/a
Supplemental requirements in addition to the Call-Off terms:	n/a
Alternative clauses:	n/a
Buyer specific amendments to/refinements of the Call-Off Contract terms:	The Supplier shall ensure that the Key Personnel listed below fulfil the Key Roles at all times during the term, The Supplier shall not remove or replace any Key Personnel unless: a) Requested to do so by HMCTS; b) The person concerned resigns, retires or dies or is on maternity or long-term sick leave c) The person's employment or contractual arrangement with the Supplier is terminated for material breach of contract by the employee; or d) The Supplier obtains HMCTS's prior written consent (such consent not to be unreasonably withheld or delayed). REDACTED
Public Services Network (PSN):	n/a
Personal Data and Data Subjects:	Confirm whether either Annex 1 or Annex 2 of Schedule 7 is being used: Annex 1

1. Formation of contract

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

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

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

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

2. Background to the agreement

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

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

Signed:	REDACTED	REDACTED
Name:	REDACTED	REDACTED
Title:	REDACTED	REDACTED
Signature:	X	X
Date:		

Schedule 1 – Services

Schedule 1 – Background

1 Scheme Overview

Under existing policy, everyone entering one of HMCTS 325 courts / tribunals buildings via public entrances is subject to a search via scanning by an archway metal detector (AMD) and/ or hand-held wand and an inspection of their bags except visiting Judicial Office Holders, police officers in uniform and armed police officers. Such access for those exempt is only permitted after the following means of strong authentication:

i. Visiting Judicial Office Holders must present an ID pass and be expected to attend a hearing, with their name on the daily list

ii. Police officers in uniform, must produce on request a warrant card or are attending a Court/Tribunal to deal with an emergency

iii. Armed police officers must have received permission to enter from the Resident Judge / District Judge / Magistrates' Chairman or Tribunal Judge

iv. Staff and judiciary, based in particular sites, can secure building-specific access passes, allowing them to enter and exit through dedicated staff entrances, and so avoiding the need to submit to security search on entry procedures via public entrances. Staff / judiciary who do not hold relevant access passes should enter buildings via public entrances and will be subject to security searches accordingly.

The Professional Users Access Scheme was developed in response to a clear perception on the part of many lawyers accessing the courts and tribunals estate in a professional capacity that security search on entry protocols are disproportionately/unduly strict.
The scheme was piloted as a proof of concept from September 2018 to November 2018. This pilot involved the testing of new streamlined processes, designed to offer exemption from searching whilst maintaining effective security to mitigate the safety risk of an imposter circumventing controls and injuring court/tribunal users with a weapon. This pilot has been fully evaluated and the results fed into the development of options for the way forward for this scheme.
At a high level the service can be summarised as the management and administration of an accredited membership database or platform, the information contained within being used and linked to create a form of access management to verify electronic IDs and grant fast track access to those accredited.

Independent bodies linked to the legal profession (such as the Bar Council) will sign up for the scheme with HMCTS, then accredit their members for scheme usage. This service will provide a central repository for all these accredited members. Independent bodies will then issue either an electronic or physical ID to accredited members, linked back to the central repository. It is estimated that there will be a minimum of 3,000 users of the scheme by the time the implementation is complete but please note that our expected user volumes do not constitute a guarantee of committed work to the supplier.

The IDs will then be verified by HMCTS Security Guards at each participating court (it is anticipated that this will be done using a hand-held device) against the data held by the supplier of those individuals accredited for fast-track access.
The anticipation of the use of hand held devices is due to the challenges HMCTS faces in implementing a standardised solution across an estates portfolio that is diverse in size, age, layout, number of entry points and listed status.
It is anticipated there will be 1-2 of these verification devices in each of our 325 court buildings. For the avoidance of doubt HMCTS will be responsible for providing these devices.

The Supplier is required to design, develop, test, implement, and administer a national roll-out of a system that will enable PUAS to all court and tribunal centres across England and Wales, and then provide on-going support (second and third line only) and maintenance to the scheme. HMCTS envisage a roll-out/implementation over a period of 3 months, with a subsequent 18-month period of maintenance and support as detailed in this requirement. The contract will also contain 2 no. 1 year extension options.

2 Expected Scheme benefits

i) Improved risk-based focus for manned guarding teams, so increasing effectiveness/performance;

ii) Improved security arrangements for legal professionals, who would no longer have to stand in line with parties on opposing sides, and so mitigate the risk of confrontations or worse on HMCTS premises;

iii) Allowing legal practitioners to access courts / tribunals more easily and without undue delay, reducing the risk of lawyers being late for conferences or hearings;

iv) Better targeting of resource on the mainstream security search on entry queues, helping to deal with them more quickly and efficiently;

v) Overall better user/stakeholder satisfaction, leading to reduced failure demand due to a reduction in complaints; and

vi) Helping to improve court/tribunal efficiency as per the above, resulting in maximisation of the value from taxpayers' money.

Schedule 1- Functional requirements

Req_Id	High Level Requirement	Comments/Example/Guidelines (New)	MoSCoW	Category	Product Supplier Notes
PUAS-FR-0001	The system must be able to record a Access Scheme User Account that will be used to validate the identity of the individual in various HMCTS locations	The data required could contain, subject to data protection constraints: First Name, Last Name, Email(s), Organisation, Contact Number(s), ID Photo, Start Date, End Date, Status, Load Date, Change History, Access History. It is expected that the Access Scheme User Account would already be validated by the organisation using their own specific workflow.	M	Access Scheme User Account Management	REDACTED
PUAS-FR-0002	The system must be able to group Access Scheme Users via organisation	Organisations include The Bar Council, Legal firms etc.	M	Access Scheme User Account Management	
PUAS-FR-0003	The system should allow for actions to be performed against an organisation and an individual account	Organisation XYZ has left the scheme and all accounts are to be suspended prior to removal	S	Access Scheme User Account Management	
PUAS-FR-0004	The system must allow the addition, modification and removal of individual Access Scheme Users via a user interface	The user interface will be accessed by both internal and external of HMCTS	M	Access Scheme User Account Management	
PUAS-FR-0005	The system must allow the addition, modification and removal of individual Access Scheme Users via an API	API will be accessed by both internal and external of HMCTS	M	Access Scheme User Account Management	
PUAS-FR-0006	The system must allow the addition, modification and removal of multiple Access Scheme Users via a user interface via a file upload	The user interface will be accessed by both internal and external of HMCTS	M	Access Scheme User Account Management	REDACTED

PUAS-FR-0007	The system must allow the addition, modification and removal of multiple Access Scheme Users via an API	API will be accessed by both internal and external of HMCTS	M	Access Scheme User Account Management	REDACTED
PUAS-FR-0008	Once processed, all changes to the Access Scheme User Account must be available immediately - See NFR for more	If a registered user account is suspended, once the account has been updated, that change will be visible. i.e. at 10:00 the account is marked as suspended. At 10:01 if the account attempts to be used, the suspended status is displayed/used by the process	M	Access Scheme User Account Management	
PUAS-FR-0009	The system should provide multiple values for the status of each Access Scheme User Account to allow for operational ease in user management	Examples are Active, Suspended, Pending Review	S	Access Scheme User Account Management	
PUAS-FR-0010	The system should provide flexible lists to Administration Users of Access Scheme User Accounts to allow for operational tasks	In addition to standard views and lists of the product	S	Usability	
PUAS-FR-0011	The system must allow the addition, modification and removal of individual Administration User via a user interface	The user interface will be accessed by both internal and external of HMCTS	M	Administration User Management	
PUAS-FR-0012	The system must allow the addition, modification and removal of individual Administration User via an API	API will be accessed by both internal and external of HMCTS	M	Administration User Management	
PUAS-FR-0013	The system should allow the addition, modification and removal of multiple Administration Users via a user interface via a file upload	The user interface will be accessed by both internal and external of HMCTS	S	Administration User Management	
PUAS-FR-0014	The system should allow the addition, modification and removal of multiple Administration Users via an API	API will be accessed by both internal and external of HMCTS	S	Administration User Management	

PUAS-FR-0015	Once processed, all changes to an Administration User account must be available immediately - See NFR for more	If a Administration Users account is suspended, once the account has been updated, that change will be visible. i.e. at 10:00 the account is marked as suspended. At 10:01 if the account attempts to be used, the suspended status is displayed/used by the process	M	Administration User Management	REDACTED
PUAS-FR-0016	The system should provide multiple values for the status of each Administration User account to allow for operational ease in user management	Examples are Active, Suspended, Pending Review	S		
PUAS-FR-0017	The system must be able to group Administration Users via organisation	Organisations include The Bar Council, Legal firms etc.	M	Access Scheme User Account Management	
PUAS-FR-0018	The system should allow for actions to be performed against an organisation and an individual account	Organisation XYZ has left the scheme and all accounts are to be suspended prior to removal	S	Access Scheme User Account Management	
PUAS-FR-0019	The system must provide a hierarchy of administrative user privileges	To enable organisations to self manage their admin users, typically a "Super" Admin user account is created that can manage other admin accounts.	M	Administration User Management	
PUAS-FR-0020	The system must provide a super user account to HMCTS to allow on-boarding and off-boarding of new organisations	HMCTS will own the process of organisations who Join and Leave the Scheme	M	Administration User Management	
PUAS-FR-0021	The system must record all actions performed on all user accounts	Recording, what account, what change, what user made the change, when, channel etc.	M	Logging	
PUAS-FR-0022	The system must provide access to the audit log as per HMCTS policies	Please see NFR's	M	Audit	

PUAS-FR-0023	The system should provide feedback to the calling system as part of the API contract	Success, failure etc.	S	Integration	REDACTED
PUAS-FR-0024	The system should provide an API to retrieve users account details	API will allow for request to specify if individual or all accounts that meet selection criteria. Access permissions will be enforced	S	Integration	
PUAS-FR-0025	The system should provide API access to all data stored within the system		S	Integration	
PUAS-FR-0026	The system must be able to record and provide access to the history of the lists of users received.	Detailing who set, when received, number of users, results of import broken down into success, failure and refer etc.	M	Reporting	
PUAS-FR-0027	The system must provide the functionality to access the other HMCTS systems via APIs, including but not limited to, the hearings management interface.	For example, to register that a user has arrived in the building.	M	Integration	
PUAS-FR-0028	The system must record the date, time and location when the Access Scheme User is requesting access to the building	In reality, this is every time the User attempts validation at the location	M	Logging	
PUAS-FR-0029	The system must record the output of any failures of the validation step when the Access Scheme User is requesting access to the building, including a reason code		M	Logging	
PUAS-FR-0030	The system must present the recent history of validation steps when the Access Scheme User is requesting access to the building to enable the HMCTS staff to see if the pass may be compromised	For example, if the Access Scheme User is reported to be at another location at the same time	M	Usability	
PUAS-FR-0031	The system could provide the ability to perform 'fuzzy' searches to find entries which nearly match the specific search query.		C	Reporting	
PUAS-FR-0032	The system must provide real-time operational reporting and dashboards for operational needs.	For example, how many Access Scheme Users have been recorded as using the system as at the time of requesting the information	M	Reporting	

PUAS-FR-0033	The system must enable all data to be extracted to be ingested with the HMCTS architecture. This includes, but is not restricted to, the strategic Data Platform for MI purposes.	This could be a PUSH or PULL approach via API or files	M	Integration	REDACTED
PUAS-FR-0034	The system must allow Administration Users to manage any static reference data internally within the system. Any changes to static data shall not have an adverse impact on existing data in the system (e.g. renaming of a Location type from "Victoria" to "HMCTS Victoria" should not impact existing sessions with the 'old' name).	For example, locations and venue names change (not the same as being a new location with a new postal address). - There will be the ability to import, create/delete, define the fields that hold the static reference data, and define the sequence of how it is presented to users. - The reference data will need to be grouped according to logical groups sub-groups and sub-sub-groups etc.	M	Reference Data	
PUAS-FR-0035	The system must have the ability to anonymise/remove personal data in the system when no longer needed for operational reasons.	For example, anonymising the names of removed users in certain displays. This does not include Audit Logs.	M	Data & Privacy	
PUAS-FR-0036	The system must provide configurable access to functions and data based on user role and group.		M	Access Management	
PUAS-FR-0037	The system must provide different levels of access to users - e.g. read-only, read/write, read/write/delete.		M	Access Management	
PUAS-FR-0038	The system must provide the ability to view a change history of entities/items undertaken on the system. The same security restrictions will be applied to historical data as to current data.	This includes but not limited to: registration requests and administrative changes such as status changes. For example, a manager wants to see who has made a status change to a Access Scheme User Account. This should be achieved without raising any service tickets or request to a third party.	M	Logging	
PUAS-FR-0039	The system must adhere to GDPR data retention requirements.	Includes anonymization of certain data elements across different tables and data purging for some data elements.	M	Data & Privacy	

PUAS-FR-0040	The system must integrate with HMCTS systems VIA API for data considered to be reference data.	For example, locations and venue names.	M	Reference Data	[redacted]

Schedule 1 – Non-Functional Requirements

Ref.	Requirement	Category	Minimum Assessment	Product Supplier Compliance Notes
PUAS-NFR-001	The system shall operate 24 hours a day, 365 days per year. There shall be equivalent availability to the Reform Technology services, thus must not have a downtime of more than one hour per quarter (being 99.8% availability over a year) - 1 hour maximum single outage, 1 hour max total outage per quarter. Other service elements only accessed during CTSC opening hours must not have downtime of more than two hours per quarter during CTSC operating hours (being an availability of 99.8% during operating hours over a year assuming operating hours as stated below in this list) - 2 hour maximum single outage, 2 hour max outage per quarter)	Reliability		REDACTED
PUAS-NFR-002	The system shall have no more than one service interrupting fault per quarter.	Reliability		
PUAS-NFR-004	There shall be no data loss or corruption during normal system activity.	Reliability	3	
PUAS-NFR-005	The supplier shall make tools available to measure availability in line with the Reliability targets specified within the NFRs.	Reliability		
PUAS-NFR-007	The supplier must have a resilience in deployment approach which means no single point of failure results in loss of service or data.	Reliability		
PUAS-NFR-008	The system shall have a recovery point objective equivalent to zero data loss. User data loss shall be restricted to uncommitted data only in the event of a failure.	Reliability		
PUAS-NFR-010	The system shall comply with GDPR (Part 3 may be relevant), National Cyber Security Centre (NCSC) guidance, and data protection policies (DPA and FoIA).	Data & Privacy	3	
PUAS-NFR-011	The data and processing elements of the system shall be within the UK (including live, test and backup data and systems).	Data & Privacy	3	
PUAS-NFR-012	The system shall provide the ability for user access to be granted or denied based on the geographical location of the user - e.g. inside the UK or other specified country.	Data & Privacy		

PUAS-NFR-013	The system shall be capable of storing all the associated data for a 12 month period and in line with the policies specified elsewhere in the NFRs. Please note that retention policies may change hence the supplier shall ensure that their solution is capable of managing increases and decreases in data retention storage requirements.	Data & Privacy		**REDACTED**
PUAS-NFR-014	The system response time for user interface interactions shall be: one second (90th percentile), 1.5 seconds (95th percentile) and two seconds (99th percentile) at the server level interaction. This shall be irrespective of the batch or background processing that may be happening in parallel.	Performance and Scalability		
PUAS-NFR-015	The system shall be capable of scaling to double normal operation (transaction volumes) during peak demand (approx 8:30-10:00am).	Performance and Scalability		
PUAS-NFR-016	When the load increases suddenly (up to double normal usage), response times shall remain unaffected or shall return to normal within 120 seconds.	Performance and Scalability		
PUAS-NFR-017	The system core operating hours shall be 9 am to 5 pm Monday to Friday.	Performance and Scalability		
PUAS-NFR-018	The system user interface shall provide feedback to the user when the processing of synchronous events exceeds two seconds.	Performance and Scalability		
PUAS-NFR-019	The system shall support at least 80% of the maximum number of concurrent users logging in within a 10 minute period without adversely impacting performance.	Performance and Scalability		
PUAS-NFR-020	The system shall be scalable to support an increase in the number of concurrent users within five working days of notice being given by the customer.	Performance and Scalability		
PUAS-NFR-021	The system shall be capable of dealing with expected number of transactions.	Performance and Scalability	3	
PUAS-NFR-022	Performance reports shall be produced weekly. These shall cover at least the following areas: · Business transaction volumes · User concurrency · System availability	Performance and Scalability		

PUAS-NFR-023	System and software upgrades shall be provided to ensure the system remains in full maintenance support throughout its life.	System and Maintenance	3	**REDACTED**
PUAS-NFR-024	Planned maintenance shall be applied to the system in a way that will negate the need for downtime.	System and Maintenance		
PUAS-NFR-025	The system will be deployed onto public cloud hosting environments, with no dependency on private infrastructure. Test / Demo Systems could be deployed on private sandbox environments.	System and Maintenance		
PUAS-NFR-026	The system shall have remote monitoring and alerting of all critical components so that the health of the system can be determined by support staff without manual intervention or reporting of issues by users.	System and Maintenance		
PUAS-NFR-027	The system shall monitor resource utilisation at defined intervals. The system shall alert the support team if utilisation is in excess of defined thresholds.	System and Maintenance		
PUAS-NFR-028	Log data of all types shall be accessible to HMCTS. The data shall be retained for up to 12 months in the system.	System and Maintenance		
PUAS-NFR-029	All expected and unexpected errors shall be logged for the purpose of dealing with incidents.	System and Maintenance		
PUAS-NFR-030	All metrics captured shall be logged and stored for 12 months for the purpose of trend analysis for both system maintenance and service management.	Service Management		
PUAS-NFR-031	It shall be possible to present each metric graphically for trend analysis using a single interface / dashboard.	System and Maintenance		
PUAS-NFR-032	It shall be possible to make new reports, views and alerts as part of continuous service improvement.	System and Maintenance		
PUAS-NFR-033	The supplier shall hold ISO 27001:2013 certification for the system(s) used for this solution and all related procedures.	Security		

PUAS-NFR-034	The supplier shall provide evidence of penetration testing on all the applications within the system within the last twelve months. The supplier shall demonstrate that no critical or high vulnerabilities exist and that any medium or low vulnerabilities are being addressed.	Security	3	**REDACTED**
PUAS-NFR-035	The supplier shall provide evidence from a third party assessor demonstrating GDPR and Law Enforcement Directorate (LED) compliance.	Security		
PUAS-NFR-036	It shall be possible to manage user permissions at a group and team level, as well as by individual user.	Security	3	
PUAS-NFR-037	The system shall allow a user to be designated as a local administrator so that they can then create further accounts within their organisation.	Security		
PUAS-NFR-038	The system shall support the use of the standard authentication protocols where required; between user to system and system to system; OAuth, SAML, SSO, CAPTCHA, KERBEROS, TLS.	Security		
PUAS-NFR-039	The software updates shall be applicable to the system and shall be sourced from an approved repository in line with the standards of the customer for the type of operating system. The patches shall be subject to integrity checking and shall be sourced from an integral source (if DNS is used to resolve the source address, authentication on responses shall be configured – e.g. DNSSEC).	Security		
PUAS-NFR-040	The system shall report security critical events to the customer's and supplier's Security Information and Event Management (SIEM) solution. The user shall be prevented from tampering with the reporting of events from the device. The logs shall be retained for 90 days minimum, except where legally they shall be kept longer in line with HMCTS retention policies.	Security		

PUAS-NFR-041	The system shall support anti-virus software (if applicable to the type of operating system) and be able to draw regular updates from an approved repository. As with other software updates, the updates shall be subject to integrity checking and DNS authentication controls. Use of the NCSC DNS if possible.	Security		**REDACTED**
PUAS-NFR-042	The system shall support applicable NCSC Cloud Security Guidance principles in any cloud service.	Security		
PUAS-NFR-043	The supplier shall verify all supplier controlled hardware (including virtual) and software configurations against unauthorised changes at least once during any period of twelve months.	Security		
PUAS-NFR-044	The supplier shall ensure segregation of duties by privileged users of the services, to ensure separation of request, approval and processing stages for account creation, changes to user permissions, account deletion, access to and processing of Protective Monitoring logs.	Security		
PUAS-NFR-045	The system shall ensure that data is encrypted by default, whether at rest within the infrastructure, in transit within the infrastructure or in transit between the infrastructure and another environment.	Security	3	
PUAS-NFR-046	The system shall be able to integrate with any IPS (Intruder prevention) and IDS (Intruder detection) systems used by the customer.	Security		
PUAS-NFR-047	The system shall perform a spam filtering function, phishing filtering function. malware filtering function - where applicable - to the solution (e.g. email handling or file uploads).	Security		
PUAS-NFR-048	The protocols used to run, gain access and support the system shall be kept to a minimum and agreed with the customer.	Security		

PUAS-NFR-049	The supplier and sub-contractors shall comply with the NCSC and HMCTS best practise and guidance unless otherwise agreed by the HMCTS Technical Decision Authority. The supplier and any sub-contractors shall comply with the following HMCTS policies: HMCTS Code of Connection HMCTS Password Policy HMCTS Patching Policy HMCTS Logging and Monitoring Policy HMCTS Operational Security Policy HMCTS Vulnerability Scanning Policy	Security	3	**REDACTED**
PUAS-NFR-050	The supplier shall ensure that services are delivered entirely from within an ISMS which is certified to ISO27001 by a UKAS registered organisation within 12 months of contract signature. The scope of the certification shall include all services and elements used in the delivery of the Services.	Security		
PUAS-NFR-051	The supplier shall provide a single point of contact for security who can attend weekly security working group meetings until full assurance of the solution.	Security		
PUAS-NFR-052	The supplier shall supply the customer with a high-level design (solution blueprint) of the solution that has been baselined and agreed with the HMCTS security team. The design shall include how the security requirements will be met.	Security	3	
PUAS-NFR-053	The supplier shall supply full ITHC (CREST or CHECK certified) results of the system and a remedial action plan for any vulnerabilities uncovered by the ITHC.	Security		
PUAS-NFR-054	Any vulnerabilities uncovered by the ITHC or further testing shall be resolved within the following periods. Critical - one week, High - two weeks, Medium and low - four weeks.	Security		
PUAS-NFR-055	The supplier shall report any possible breach of the customer's data within 24 hours of the incident.	Security		
PUAS-NFR-056	The supplier shall ensure that all changes to services impacting IT security apply the agreed change procedure and take account of the latest Security Aspects Letter (SAL).	Security		
PUAS-NFR-057	The supplier shall provide certificates of decommissioning to the customer, These certificates shall have been signed by a member of supplier staff with suitable legal and commercial authority - e.g. hardware, environments, servers and data	Security		

PUAS-NFR-058	The supplier shall provide evidence to the customer accreditor that the physical security of sites hosting customer assets is appropriate. Physical security shall be assessed using appropriate methodologies (e.g. those provided by CPNI) as agreed with the HMCTS security team.	Security		**REDACTED**
PUAS-NFR-059	The supplier shall ensure that all supplier and sub-contractor staff who have access to personal data, including staff in their supply chain if appropriate, undergo a session of information risk awareness training on induction and annually thereafter.	Security		
PUAS-NFR-060	The supplier shall produce and maintain an accurate inventory of information, system, hardware (where applicable) and software assets used to deliver the services (the "Information Asset Database" and the "Equipment Asset Database" and together with the "Asset Databases").	Security		
PUAS-NFR-061	The supplier shall prepare, develop, maintain and deliver to the customer for approval a complete and up to date Security Management Plan covering all services delivered under this contract, within 20 working days after the commencement date. The Security Management Plan shall be structured in accordance with ISO27001 and ISO27002 and conform to the general obligations set out in the HMG IA standards.	Security	3	
PUAS-NFR-062	The supplier shall ensure, and provide evidence to the customer, 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.	Security	3	
PUAS-NFR-063	The supplier shall apply a patch immediately if the infrastructure for which they are responsible suffers from a vulnerability that is being exploited elsewhere.	Security	3	
PUAS-NFR-064	The supplier shall have a protective monitoring policy to assist in identifying security incidents quickly and to provide the customer with information that will assist in initiating the incident response policy as early as possible.	Security	3	
PUAS-NFR-065	Any vulnerabilities uncovered by the ITHC or further testing shall be resolved within set periods to be agreed with HMCTS.	Security		
PUAS-NFR-066	Supplier support staff shall be located within the UK where possible. Support staff can be located outside the UK with the agreement of the customer.	Security		
PUAS-NFR-067	The supplier is not permitted to extract / export any data without written consent from the customer.	Security	3	

PUAS-NFR-068	Data in any non-production environment shall not contain live data without prior approval from the customer.	Security	3	**REDACTED**
PUAS-NFR-069	The supplier shall hold ISO IEC 20000-1:2018 certification, or equivalent, for the management of the end to end services being provided. This shall include all related processes prior to service go-live, acceptance into service and formal acceptance / sign-off by the customer.	Service Management		
PUAS-NFR-070	The supplier shall develop and maintain a complete and up to date service management plan, The plan and changes shall be approved by the customer. The plan shall cover all services delivered under this contract, within twenty working days after the commencement date. The service management plan shall be structured in accordance with ISO20000-1:2018 standards or equivalent.	Service Management		
PUAS-NFR-071	The supplier shall provide a Service Desk capability to support the customer's core operating hours from the UK only, with the possibility of flexing to additional service hours without employing "follow the sun" support.	Service Management	3	
PUAS-NFR-072	The supplier shall provide a Service Desk to act as a single point of contact for the customer or its representative. The Service Desk shall ensure that issues are resolved, and provide information on the impact of planned changes and unplanned events.	Service Management	3	
PUAS-NFR-073	The customer shall provide in-house support of as described in the 'Support Services' tab and to the resolution and response times detailed in the 'SLA' tab.	Service Management	3	
PUAS-NFR-074	The supplier shall provide to the customer the resources and access level needed to deliver their support line responsibilities as detailed in the 'Support Services' tab.	Service Management	3	
PUAS-NFR-075	The supplier shall use the incident classifications as listed in the 'SLA'tab. Exact wording maybe amended to suit the successful supplier but should not be materially changed.	Service Management	3	
PUAS-NFR-076	The supplier shall, within the core operating hours, deal with all incidents in accordance with the service levels specified for each priority level in the 'SLA' tab.	Service Management	3	

PUAS-NFR-077	The supplier shall work collaboratively with HMCTS to provide a seamless, integrated, end to end service. The supplier shall support the customer or its representative in the development and implementation of an Operational Working Agreement (OWA) defining the responsibilities and relationships between the various parties involved in delivering the end to end service.	Service Management	3	**REDACTED**
PUAS-NFR-078	The supplier shall provide all relevant service consumption information to the customer or its representative.	Service Management		
PUAS-NFR-079	The supplier shall conduct proactive monitoring to identify any emergent risk to the provision of the services and report these immediately to the customer or its representative.	Service Management	3	
PUAS-NFR-080	The supplier shall implement measures to address an emerging risk when requested by the customer or its representative. These measures shall be agreed with the customer and then implemented within 20 working days.	Service Management		
PUAS-NFR-081	The supplier shall analyse incidents to find patterns that identify common underlying causes (Problem Management). The supplier shall use a process which is auditable against ITIL v3 Service Management good practice or equivalent practice as appropriate.	Service Management		
PUAS-NFR-082	The supplier's handling and implementation of Change Requests shall be subject to a management process that provides the customer with appropriate control of expenditure, risk, implementation of policies and strategy (Change Management). The supplier shall use a process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate	Service Management		
PUAS-NFR-083	The supplier shall raise requests with the customer for Changes. These shall include (but are not limited to) Operational Changes, Standard Changes and Emergency Changes.	Service Management		
PUAS-NFR-084	The supplier shall receive Change Requests from the customer or its representative and shall provide them with an Impact Analysis on the request within five working days.	Service Management	3	
PUAS-NFR-085	The supplier shall ensure that all Requests for Change they submit to the customer contain at least the following information (i) Verified Implementation Plans (ii) Post Implementation Review (iii) Acceptance Criteria (iv) Back Out Plans or Remediation Plans (v) Plans for handover to support (vi) Evidence of successful test activity	Service Management	3	

PUAS-NFR-086	The supplier shall control, track and record the existence and configuration of assets involved in the delivery of services so that the supplier and customer can maintain their ability to manage the service (Configuration Management). The supplier shall use a process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate.	Service Management		**REDACTED**
PUAS-NFR-087	The supplier shall manage changes to the platform and applications under a process that is designed to minimise risk and the impact on normal service (Release Management). The supplier shall use a process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate.	Service Management		
PUAS-NFR-088	The supplier shall produce, maintain and assure up-to-date information for inclusion in the Supplier's Knowledge Management System, to include but not limited to: (i) Methods to resolve Incidents; (ii) Known errors (iii) Service Desk scripts (iv) Self-help articles (v) Frequently Asked Questions (FAQs).	Service Management		
PUAS-NFR-089	The supplier shall produce reports that allow the customer and the supplier to jointly manage the performance of the Service. A mechanism shall be implemented to provide a regular review of Service Levels, and implementation of plans for improving these where agreed (Service Level Management) using a process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate.	Service Management		
PUAS-NFR-090	The supplier shall be able to predict usage of resources on which the delivery of the services depends, and Change Requests raised by the Customer, to avoid the situation where a resource is exhausted (Capacity Management). The supplier shall use a process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate.	Service Management		
PUAS-NFR-091	The supplier shall develop and maintain plans for providing the required level of continuity of services following incidents that have a significant impact (Service Continuity Management). The supplier shall use a process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate.	Service Management		

PUAS-NFR-092	The supplier shall support the customer, or its representative, in undertaking an annual review (or a review post-invocation) of the IT Service Continuity Management (ITSCM) plan and associated processes. Typically Monthly Service Meetings will highlight any gaps in the process.	Service Management		**REDACTED**
PUAS-NFR-093	The supplier shall be responsible for the ongoing management and monitoring of licence usage, within their services, to ensure that it is both legal and efficient. This shall include the enablement of licence re-deployment to minimise licence costs if applicable.	Service Management	3	
PUAS-NFR-094	The supplier shall ensure that service reports include at least the following: Executive Summary Dashboard views of the performance data Performance against all KPIs/Performance Measures User statistics – by court, professional body, date and time Number of failed access attempts and reasons Full Details of any Priority 1 and Priority 2 Incidents (or associated problem records) logged Overall % of Performance Measures Met % of Performance Measures Missed more than once % of Incidents Re-opened Number of Problem Records Opened Number of Problem Records Closed Number of Changes Number of Failed Changes Number of Security Incidents	Service Management	3	
PUAS-NFR-095	The supplier shall identify improvement initiatives that deliver end-to-end, measurable and sustainable benefits to the customer. The supplier shall use a Continuous Service Improvement (CSI) process which is auditable against ITIL V3 Service Management good practice or equivalent practice as appropriate.	Service Management		
PUAS-NFR-096	The supplier shall provide a single point of contact for service management, and escalation of issues, who shall - attend meetings and management groups as appropriate; and - have oversight of the entire service provision; and - understand the whole process including interfaces with other parties.	Service Management	3	

PUAS-NFR-097	The supplier must work in a collaborative way with HMCTS and independent bodies to ensure the service provision is efficient and effective.	Service Management	3	**REDACTED**
PUAS-NFR-098	The supplier should work in an open and transparent manner with HMCTS.	Service Management		
PUAS-NFR-099	The supplier should work with HMCTS and independent parties to improve the quality of the service and increase the number of participants.	Service Management		
PUAS-NFR-100	Following Scheme go-live the supplier must facilitate (provision, organise and document) a monthly operations meeting with HMCTS representatives. Every third meeting shall be expanded to encompass any commercial/contractual issues.	Service Management	3	
PUAS-NFR-101	The supplier could be required to attend ad-hoc operational meetings involving the independent bodies or other parties, and should provide representation as requested.	Service Management		
PUAS-NFR-102	The supplier must be responsible for the effective delivery of the transition from the current system to the new system including collaboration and conflict resolution with the incumbent supplier.	Service Transition	3	
PUAS-NFR-103	The supplier must create and maintain a project plan (showing all parties and their tasks) showing current status and any slippage for the transition from the existing system to the new system, including implementation of the new system.	Service Transition	3	
PUAS-NFR-104	The supplier must be able to deliver the implementation and be ready to go live by the end of July. At go-live the scheme shall support the number/level of courts currently covered by our existing scheme (95 courts) and then roll out to cover the remaining estate within the following 3-4 months.	Service Transition	3	
PUAS-NFR-105	The supplier shall provide a single point of contact responsible for service transition/implementation.	Service Transition	3	
PUAS-NFR-106	The supplier shall provide technical and operational documentation to enable support functions to manage the service. The documents shall describe in sufficient detail how all ITIL disciplines will operate in the BAU support model. The contents of these documents shall be tested, approved and baselined. They will be made available to all support teams in the agreed repository prior to service rehearsals and service commencement.	Service Transition	3	

PUAS-NFR-107	The supplier shall provide evidence that the system is operable and meets agreed expectations for its operation prior to the commencement of live service, as set out in the Acceptance Into Service checklist agreed between the supplier and customer	Service Transition	3	**REDACTED**
PUAS-NFR-108	The supplier shall provide evidence that the system meets its defined accessibility requirements and follow any agreed design standard, prior to the commencement of live service. Any assistive technology requirements will have been defined, delivered and tested as set out in the Acceptance into Service checklist agreed between the supplier and customer.	Service Transition		
PUAS-NFR-109	The supplier shall provide a user interface (UI) and user experience that follows the Government Digital Service (GDS) design standards as far as practical / appropriate in the context of this solution.	Usability & Accessibility		
PUAS-NFR-110	The system shall demonstrate appropriate consideration of how user errors can be corrected. Examples include: - A user shall be able to 'undo' and 'redo' actions. - 'Destructive' actions shall require double confirmation. - It shall be possible to specify data validation rules - e.g. a date field may only contain a date in a specified format.	Usability & Accessibility		
PUAS-NFR-111	The system shall include appropriate error management (error prevention, error correction, error messages). The system shall employ sound validation policies reducing unnecessary re-work and aiding usability. Error messages shall be clear, informative, correct and non-terminal (i.e. error trapping code should facilitate users' ability to return to a known safe operational state as far as possible).	Usability & Accessibility		
PUAS-NFR-112	The supplier shall make an assessment to determine if the system has sufficient capacity for the expected load prior to the commencement of live service. The impact of the new capability on the capacity of networks, infrastructure or other shared components that it relies upon shall also be considered.	Service Transition	3	
PUAS-NFR-113	The supplier shall provide evidence that availability targets are set and monitoring in place to report levels actually achieved prior to the commencement of live service.	Service Transition	3	
PUAS-NFR-114	The supplier shall provide data management documentation prior to the commencement of live service. This shall include data migration, archiving and deletion, and any reliance on data from other systems.	Service Transition	3	

PUAS-NFR-115	The supplier shall document all batch, system, operational and interface processes (including the technical components and the support arrangements). This also includes the recording of Event Logs and Error Logs, Defined Scheduled Jobs, Controlled and Logged Processes, Process Durations and any Automated & Manual Processes.	Service Transition		**REDACTED**
PUAS-NFR-116	The supplier shall provide evidence that the system is capable of meeting the specified service performance requirements. The factors that could affect performance shall be known and the ceiling limits for these factors will be documented.	Service Transition	3	
PUAS-NFR-117	The supplier shall provide the customer with a high level design of the Service Model that has been agreed with HMCTS DCD Digital Operations. The design shall include how the service requirements shall be met.	Service Transition	3	
PUAS-NFR-118	The supplier shall provide the cost model and associated artefacts for billing and invoicing of the service to HMCTS DCD prior to commencement of the Live Service.	Service Transition		
PUAS-NFR-119	The supplier shall work with the customer to agree and document a supplier management strategy, approach and process. This shall include (but not be limited to) escalation matrices, contact routes and handovers to suppliers which is to be fully tested prior to Live service commencement.	Service Transition		
PUAS-NFR-120	The supplier shall agree with the customer and document all arrangements for Incident Management and Major Incident Management. This includes (but is not limited to) minimum data set, priority definitions, outage communications and user types.	Service Transition	3	
PUAS-NFR-121	The supplier shall provide evidence that documentation relating to any existing problems or known errors has been transferred to the Problem Management team prior to the commencement of Live Service.	Service Transition	3	
PUAS-NFR-122	The supplier shall work with the customer to ensure that the change and release arrangements are defined and approved pre go live.	Service Transition	3	
PUAS-NFR-123	The supplier shall work with the customer to ensure that the end to end request process is documented, including approvers, licence management and logistics. Common requests shall be added to the service catalogue and provision made for users to use this request route.	Service Transition	3	

PUAS-NFR-124	The supplier shall work with the customer to ensure that there is a plan for knowledge transfer for all relevant service teams and evidence that knowledge articles have been created.	Service Transition	3	**REDACTED**
PUAS-NFR-125	The supplier shall provide evidence of their compliance to the joiners, movers and leavers processes prior to the commencement of live service. All user and support accounts shall be Role Based Access Control (RBAC) based. Prior to the commencement of live service, project teams should expect to lose any privileged accesses. The role of any functional mailboxes shall also be documented and included in the agreed Service Design.	Service Transition	3	
PUAS-NFR-126	The supplier shall provide support and resourcing as part of Early Life Support for a period to be agreed with the customer which could include the provision of floorwalkers on-site.	Service Transition	3	
PUAS-NFR-127	The supplier shall provide evidence that the agreed Monitoring and Alerting is in place prior to the commencement of Live Service. This shall include (but not be limited to) that for security, performance, capacity and environment monitoring where appropriate.	Service Transition	3	
PUAS-NFR-128	The supplier shall provide documentation for recovery procedures, responsibilities and the escalation paths to be followed. The supplier shall provide test results for a partial and complete failure of the environment.	Service Transition	3	
PUAS-NFR-129	The supplier shall document their role(s), if any, in Data Migration and confirm that all their data migration tasks have been completed prior to the commencement of Live Service.	Service Transition	3	
PUAS-NFR-130	The supplier shall follow the Customer's Service Transition and Service Introduction processes.	Service Transition		
PUAS-NFR-131	The supplier shall produce a Supplier Test Policy document. This shall describe how the supplier tests the system [releases] and shall be agreed with the customer as appropriate.	Service Management	3	
PUAS-NFR-132	The system shall support bespoke development work by the supplier for full customisability of all aspects of functionality.	Supportability	3	
PUAS-NFR-133	The system shall provide the facility for extension and customization by HMCTS or third parties through an appropriate plugin architecture, or equivalent technical approach.	Supportability		
PUAS-NFR-134	The system shall provide access to all data and functionality through a set of industry standard language and platform independent APIs.	Supportability	3	

PUAS-NFR-135	The system shall provide a comprehensive set of language and platform independent events or notifications to enable event-driven integration with other HMCTS systems.	Supportability		REDACTED
PUAS-NFR-136	The supplier shall provide training to service management staff for all releases. For new products and services, this shall be prior to implementation. Any major change/Release needs to be notified three months in advance.	Supportability	3	
PUAS-NFR-137	The supplier shall provide training material to each user covering the main points of the training syllabus at least four weeks in advance of actual User Acceptance Testing (UAT).	Supportability	3	
PUAS-NFR-138	The supplier shall provide documentation that HMCTS can use to create e-learning products to train operational users of the system.	Supportability	3	
PUAS-NFR-139	The supplier shall provide training documentation to each user during any major rollout or change in the existing system. This will cover the main points of the impact from the HMCTS standpoint. Timescales will be agreed with HMCTS on a case by case basis, and be proportionate to scale and/or complexity.	Supportability	3	
PUAS-NFR-140	The system shall expire any session cookie immediately upon either the user logging out, closing the browser or upon reaching the application timeout period, forcing the user to re-authenticate.	Data & Privacy	3	
PUAS-NFR-141	The system shall have the ability to force an application timeout - which shall be configurable - to ensure applications shall not be left available and unattended.	Data & Privacy	3	
PUAS-NFR-142	The supplier shall provide clear onboarding and offboarding options and support that facilitates a move to another service provider if required.	Service Transition	3	
PUAS-NFR-143	The system shall be compliant with the versions of the browsers specified in the GDS service manual at https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices	Compatibility		

PUAS-NFR-144	The system shall have the capability to extend across different device types, such as tablets or smartphones.	Compatibility		REDACTED
PUAS-NFR-145	The system shall utilize open source products wherever possible.	Architecture		
PUAS-NFR-146	The system shall be able to support the number of transactions with other external systems based on expected use.	Capacity	3	
PUAS-NFR-147	The system shall support at least the number of expected registered users.	Capacity	3	
PUAS-NFR-148	The supplier shall be able to demonstrate that the system is inherently 'scalable'.	Capacity	3	
PUAS-NFR-149	The supplier shall carry out maintenance activities outside of core operating hours, with the agreement of the customer. The supplier shall give at least 10 working days notice.	Reliability	3	
PUAS-NFR-150	The supplier shall provide an environment(s) - for multiple parallel running projects - to perform: - Acceptable integration, - Configuration (if applicable) - Testing (if applicable) - Non-functional & User Acceptance Testing and - Training In addition to the above, in the case of the performance test environment, this shall be a scaled representation of the Live environment.	Performance and Scalability	3	
PUAS-NFR-151	The system shall audit all the following operations: create, update, delete, search parameters used, and export.	Audit		
PUAS-NFR-152	The audit function shall capture as a minimum: - the items of data being modified - the new value - the user modifying the data - the date time stamp	Audit	3	
PUAS-NFR-153	The system shall be able to present audit data to users with the appropriate security permissions.	Audit	3	

PUAS-NFR-154	The system shall ensure that a transaction (together with the log of such) cannot be tampered with once it is closed. The integrity of records of individual applicants' transactions shall be maintained.	Audit	3	**REDACTED**
PUAS-NFR-155	The supplier shall ensure that the customer is allowed access, on request, to all the outlets to conduct on-site inspections for the purpose of fraud prevention, security policy and security requirements, and compliance monitoring.	Physical Security		
PUAS-NFR-156	The customer shall be entitled at any time and without giving notice to the supplier to carry out such Security Tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Supplier's compliance with and implementation of the Security Plan. The customer may notify the supplier of the results of such tests after completion of each test.	Physical Security		
PUAS-NFR-157	The system's disaster recovery capability shall be equal to the application's live capability both in terms of access to the data and capacity, dependant on the commercial impact to the TCO.	Disaster Recovery		
PUAS-NFR-158	The supplier shall take a full system backup at least every 24 hours. It shall be stored in a secured standard open data format, in a separate location, typically offsite, that complies with all relevant security standards.	Disaster Recovery		
PUAS-NFR-159	The system backups shall be tested at least quarterly to validate backup consistency. through a full backup restoration exercise. – This will vary dependant on the architecture reference design and commercial model.	Disaster Recovery		
PUAS-NFR-160	The system shall allow external services to integrate with it via RESTful calls, authenticated and authorized using the HMCTS identity access management solution.	Architecture		
PUAS-NFR-161	The system shall make log, audit and reporting data available via RESTful APIs.	Architecture		

PUAS-NFR-162	The system shall not require the installation of an executable on the desktop.	Architecture		**REDACTED**
PUAS-NFR-163	The system shall not require the use of browser plug-ins.	Architecture		
PUAS-NFR-164	All functionality accessible through common technical integration points to enable external clients or automation. (Everything a user can do can also be done through an API.)	Architecture	3	
PUAS-NFR-165	All customer data that is decommissioned or destroyed (e.g. when the data retention period has expired) must include the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography, and/or data overwriting methods consisting of at least three complete overwrite passes of random data.	Security		
PUAS-NFR-166	At the end of the contract it must be possible for the customer to retrieve all of its data from the system in a common format (e.g.CSV, XML, JSON) and the supplier shall support the export of such data. Upon receiving such a retrieval request from the customer, the supplier shall reply within 10 working days and complete the export within 20 working days.	Data & Privacy	3	
PUAS-NFR-167	All data and statistics available via dashboards and reports must also be available via API or on-demand and regular scheduled data export in a common format (e.g.CSV, XML, JSON)	System and Maintenance		
PUAS-NFR-168	The system shall export data in a machine readable format, (e.g. CSV, XML, JSON) with the purpose of archiving externally to the system	Data & Privacy	3	
PUAS-NFR-169	The solution will employ error-handling so as to reduce to negligible, the likelihood that any operation will result in the application itself or any COTS products, browsers, etc that use it generating an unhandled exception (e.g. System crash). The solution will provide administrators with appropriate alerts and well-defined steps to recover consistently from unhandled exceptions in the processing of events.	Usability & Accessibility		

PUAS-NFR-170	The system shall follow the HMCTS minimum branding guidelines.	Usability & Accessibility		REDACTED
PUAS-NFR-171	The supplier shall optimise the accessibility of the system for disabled and other users, within the system and / or through compatibility with assistive technology. Actions and changes to achieve this shall be taken where reasonable and proportionate, as agreed with the customer. The standard of accessibility shall be informed by the Government Digital Service (GDS) service standard, Web Content Accessibility Guidelines (WCAG 2.1) and the Public Sector Equality Duty (as set out in the Equality Act 2010).	Usability & Accessibility		
PUAS-NFR-172	The system shall supports and guides the user in learning to use the system, for example by providing optional prompts to the user. Help and guidance in the system shall be provided in context (relative to the functionality the user is using) rather than in separate Help documentation.	Usability & Accessibility		
PUAS-NFR-173	The Help & Guidance content shall be managed and controlled by HMCTS	Usability & Accessibility		

Schedule 1 – Support Services

As per NFR PUAS-090, in providing support to the system the supplier will be required to liaise with a number of different HMCTS teams including:

1 HMCTS - Digital Support Officers (DSO's)

HMCTS has a network of Digital Support Officers (DSO's) who will complete an initial issue triage and resolution of incidents if possible. If they are unable to resolve, they will raise an incident with the HMCTS IT Service Desk. Typical activity includes:

i. Initial issue triage and resolution
ii. Raise incidents with DCD IT Service Desk
iii. Onsite liaison for incident resolution
iv. Support Security Guards with Failed Feed, Failed Scan, Supplier App issues, Hardware Issues and Training
v. Raise Incidents with IT Service Desk with Failed Feeds, Failed Scan, Supplier App Issues and Hardware Issues
vi. Raise Wi-Fi issues with the appropriate supplier Assist PUAS Project Team with Site Deployment and Device Set Up
vii. Report Hardware Device Security Issues (lost, stolen or compromised device) to the IT Service Desk

2 HMCTS – PUAS Project Team

The Project Team will coordinate site deployment and device set up and interact with the HMCTS IT Service Desk on hardware issues, deployment issues, email set up and hardware asset management.

Please note that this support will only be provided during the implementation period and not once the scheme has gone live. Typical activity includes:

i. Coordinate Site Deployment and Device Set Up working with DSOs
ii. Interact with IT Service Desk on Hardware Issues, Deployment Issues, Email or account Set Up (if required), Hardware Asset Management
iii. Interact with the Supplier on Membership Database and Site Set Up
iv. Respond to Hardware Device Security Issues (lost, stolen or compromised device) as required

3 HMCTS – IT Service Desk

IT Service Desk will act as single point of contact for Access Management issues identified by Digital Support Officers with the access management element of the PUAS. Typical activity includes:

i. Act as single point of contact for Access Management issues identified by DSOs with the Access Management element of the PUAS.
ii. Log tickets within ServiceNow with a unique reference number including the:
iii. Capture of the Minimum Dataset.
iv. Performance of an initial triage activity to identify the appropriate resolver.
v. Routing of tickets to the appropriate resolver, dependent on the issue that has been reported.
vi. Capture of the unique reference number for the issue from other resolver teams (if not on ServiceNow) and the recording of this reference within the ServiceNow incident record.

vii. Assignment of ticket to appropriate 'Third Party' group within ServiceNow whilst awaiting feedback from that resolver group.
viii. Where required, coordinate resolution activities between resolver groups and the requester.
ix. Support DSOs with Failed Feeds, Failed Scan, Supplier App Issues and Hardware Issues
x. Interact with the Supplier on Failed Feeds, Failed Scan (other) and Supplier App issues
xi. Interact with PUAS Project Team on Hardware Issues, Deployment Issues, Email Set Up, Hardware Asset Management
xii. Support other teams with email account creation and management for handheld access devices.
xiii. Respond to Hardware Device Security Issues (lost, stolen or compromised device) by coordinating incident resolution and blocking email accounts.

4 Independent Bodies

User Administrations will be the first point of contact for their PUAS users. Typical activity includes:

i. Acting as first point of contact for users on issues such as registration, user removal and invalid ID errors
ii. Liaising with the Supplier for Registration Portal issues and invalid ID errors as required.
iii. Liaising with the Supplier for errors in the supplier database.

5 Responsibilities

Below is a table of typical support issues detailing the responsibilities for each line of support.

Activity	Activity Type	1st Line	2nd Line	3rd Line
Site set up in ID Database	Deployment	PUAS Project Team	**Supplier**	
Hardware fulfilment to site	Deployment	PUAS Project Team	DSOs	
HMCTS Email address set up (if required)	Deployment	PUAS Project Team	IT Service Desk	
Device set up (configuration)	Deployment	PUAS Project Team & DSOs	**Supplier** PUAS Project Team	
Hardware deployment on site	Deployment	DSOs		
Training of Security Guards	Deployment	PUAS Project Team		
User registration	User Administration	Independent Bodies (e.g. Bar Council)	**Supplier**	

User removal (leavers)	User Administration	Independent Bodies	**Supplier**	
Loss of user device or electronic ID	User Administration	Independent Bodies	**Supplier**	
Registration Portal Issues	User Administration	Independent Bodies	**Supplier**	
Invalid ID errors	User Administration	Independent Bodies	**Supplier**	
On Site Triage	Access Management	DSOs	IT Service Desk	PUAS Project Team **Supplier**
Incident Raising	Access Management	DSOs	IT Service Desk	
Incident Management	Access Management	IT Service Desk	**Supplier** PUAS Project Team	
Hardware Asset Management	Access Management	DSOs	IT Service Desk	PUAS Project Team
Hardware Break/Fix	Access Management	DSOs	IT Service Desk	PUAS Project Team
Failed Scan – invalid ID	User Administration	Independent Bodies	**Supplier**	
Failed Scan – other	Access Management	IT Service Desk	**Supplier**	
Visit Sync Failure	Access Management	**Supplier**	IT Service Desk	DSOs
ID Feed Failure	Access Management	DSOs	IT Service Desk	**Supplier**
Supplier App Issues	Access Management	DSOs	IT Service Desk	**Supplier**

Hardware Device Security Issues (lost, stolen or compromised device)	Access Management	DSOs	IT Service Desk	HMCTS DACS Security Team
				Supplier
				PUAS Project Team
Supplier Membership database Issues	User Administration	Independent Bodies	**Supplier**	

Schedule 1 – SLA's

SLA - IT system failure severity and resolution table

Priority	Definition	Response Target	Resolution Target
1	• Significant service disruption or outage • Significant impact on service being provided to multiple users or locations • Any loss of service or functionality affecting all users meaning that no access to services or applications can be processed.	30 Minutes then hourly updates	8 working hours
2	Service Element Description • Functionality / performance of the service is significantly degraded / impaired and has material impact on the ability to use the system. • An infrastructure failure that leads to reliance on a single point of failure. • An Element of a service is unavailable • Can include any loss of service or functionality	1 hour then updates mutually agreed at time of call	12 working hours
3	• Multiple users report the service unavailable or partially impaired. • Functionality/performance is degraded/impaired but can be circumvented. • Non-system critical issues where a minor Incident that does not generate processing failures for users or departments but affects part of the functionality intermittently, or has potential for minor impact on the service	4 hours then updates mutually agreed at time of call	24 working hours
4	• Password Resets or single user access issues • Issues for individual users / Single User Faults • Non-technical enquiry • The Service / systems are not down or degraded. • Service Requests that are currently being provisioned via the incident module • The service is working as per design / there is no technical fault	Next business day	70 working hours

Schedule 1 – KPI's

BAU Key Performance Indicators

No	KPI Title	Definition	Freqeuncy of Measurement	Severity Levels		Service Points
1	System Availability	Calculated as = (MP-SD) x 100/MP Where: MP = total number of minutes, excluding permitted maintenance, within the month; and SD = total number of minutes of service downtime, excluding permitted maintenance, within the month	Per month	Target Performance Level	99.80%	0
				Minor KPI Failure	99.3%-99.79%	0.5
				Serious KPI Failure	98.80%-99.29%	1
				Severe KPI Failure	98.30%-98.79%	1.5
				KPI Service Threshold	below 98.29%	2
2	System Response Times	Benchmark testing of the system response time for user interface interactions irrespective of the batch or background processing that may be happening in parallel.	Exact sample number and type of tests to be confirmed with the successful supplier)	Target Performance Level	up to 1 second	0
				Minor KPI Failure	1.01-1.25 seconds	0.5
				Serious KPI Failure	1.26-1.50 seconds	1
				Severe KPI Failure	1.51-2.00 seconds	1.5
				KPI Service Threshold	under 2.00 seconds	2
3	Fix Times Priority 1 Service Incident	The incident resolution time (in operational hours) from the time the service incident is reported to the supplier, for each Priority 1 service incident.	Per incident.	Target Performance Level	up to 8 hours	0
				Minor KPI Failure	between 8hrs 1 min and 9 hrs	1

		Resolution means that either: a) the root cause of the service incident has been removed/ and the services are being provided in accordance with the Schedule 1- Services; or b) HMCTS has been provided with a workaround in relation to the service incident deemed acceptable by HMCTS		Serious KPI Failure	between 9hrs 1 minute and 10 hours	1.5
				Severe KPI Failure	between 10 hrs 1 min and 11 hrs	2
				KPI Service Threshold	over 11 hours	2.5
4	Fix Times Priority 2 Service Incident	The incident resolution time (in operational hours) from the time the service incident is reported to the supplier, for each Priority 2 service incident. Resolution means that either: a) the root cause of the service incident has been removed/ and the services are being provided in accordance with the Schedule 1- Services; or b) HMCTS has been provided with a workaround in relation to the service incident deemed acceptable by HMCTS	Per incident.	Target Performance Level	up to 48 hours	0
				Minor KPI Failure	between 48hrs 1 min and 56 hrs	1
				Serious KPI Failure	between 56hrs 1 min and 68 hrs	2
				Severe KPI Failure	between 68 hrs 1 min and 72 hrs	3
				KPI Service Threshold	Over 72 hours	4
5	Fix Times Priority 3 Service Incident	The incident resolution time (in operational hours) from the time the service incident is reported to the supplier, for each Priority 3 service incident. Resolution means that either: a) the root cause of the service incident has been removed/ and the services are being provided in accordance with the Schedule 1- Services; or b) HMCTS has been provided with a workaround in relation to the service incident deemed acceptable by HMCTS	% of Priority 3 Service Incidents resolved within 4 working days.	Target Performance Level	85%	0
				Minor KPI Failure	80-84.9%	0.5
				Serious KPI Failure	75-79.9%	1
				Severe KPI Failure	70-74.9%	1.5
				KPI Service Threshold	Under 70%	2
6	Fix Times Priority 4 Service Incident	The incident resolution time (in operational hours) from the time the service incident is reported to the supplier, for each Priority 4 service incident. Resolution means that either: a) the root cause of the service incident has been removed/ and the services are being provided in	% of Priority 4 Service Incidents resolved within 7 working days.	Target Performance Level	85%	0
				Minor KPI Failure	80-84.9%	0.25
				Serious KPI Failure	75-79.9%	0.5

		accordance with the Schedule 1- Services; or b) HMCTS has been provided with a workaround in relation to the service incident deemed acceptable by HMCTS		Severe KPI Failure	70-74.9%	0.75
				KPI Service Threshold	Under 70%	1

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:

Schedule 2 – Total Cost of Ownership

Implementation

		No. of Days					
Role	Day rate	Discovery	Design	Build	Test	Implement to 95 courts	Implement to remaining courts
Follow	REDACTED						
Assist							
Apply							
Enable							
Ensue/Advise							
Initiate/Influence							
Set Strategy/Inspire							
	Sub-Total						
	TOTAL						£50,900.00

BAU

	Number of PUAS Scheme Members					
Number of HMCTS Security Users	<3000	3000-9999	10000-14999	15000-19999	20000-24999	>25000
<250	2,150.00	2,150.00	2,150.00	2,150.00	2,150.00	2,450.00
250-349	2,400.00	2,400.00	2,400.00	2,400.00	2,400.00	2,700.00
350-449	2,900.00	2,900.00	2,900.00	2,900.00	2,900.00	3,200.00
450-549	3,400.00	**3,400.00**	3,400.00	3,400.00	3,400.00	3,700.00
550-600	3,750.00	3,750.00	3,750.00	3,750.00	3,750.00	4,050.00
>600						

Any additional integrated systems will incur an additional cost of £200 per month

Exit Costs

Fixed cost to cover **all** relevant activity (handover, data transfer, etc) required by clause 21 and to transfer the service to a new provider should this be required.

2500

TCO VALUE= **£216,600.00**

Schedule 2- Day Rates

These day rates shall be used as the basis to calculate the value of any additional work.

			Strategy & Architecture	Business change	Solution development & Implementation	Service Management	Procurement & management support	Client interface	Average
Roles	1	Follow	REDACTED						
	2	Assist							
	3	Apply							
	4	Enable							
	5	Ensue/Advise							
	6	Initiate/Influence							
	7	Set Strategy/Inspire							

Day rates are defined as:

- 8 hours work exclusive of travel and lunch
- Covering Monday - Friday excluding national holidays
- Covering office hours of 09:00 - 17:00
- Inclusive of Professional Indemnity Insurance
- Inclusive of travel, subsistence and mileage within London

Role Definitions

`

			Autonomy	Influence	Complexity	Business Skills
Roles	1	**Follow**	Works under close supervision. Uses little discretion. Is expected to seek guidance in expected situations.	Interacts with immediate colleagues.	Performs routine activities in a structured environment. Requires assistance in resolving unexpected problems.	- uses basic information systems and technology functions, applications and processes - demonstrates an organised approach to work - learns new skills and applies newly acquired knowledge - has basic oral and written communications skills - contributes to identifying own development opportunities
	2	**Assist**	Works under routine supervision. Uses minor discretion in resolving problems or enquiries. Works without frequent reference to others.	Interacts with and may influence immediate colleagues. May have some external contact with customers.	Performs a range of varied work activities in a variety of structured environments.	- understands and uses appropriate methods, tools and applications - demonstrates a rational and organised approach to work - is aware of health and safety issues - identifies and negotiates own development opportunities - has sufficient communication skills for effective dialogue with colleagues - is able to work in a team - is able to plan, schedule and monitor own work within short time horizons - absorbs technical information when its presented systematically and applies it effectively

3	**Apply**	Works under general supervision. Uses discretion in identifying and resolving complex problems and assignments. Usually receives specific instructions and has works reviewed at frequent milestones. Determines when issues should be escalated to a higher level.	Interacts with and fluence immediate department/project team members. May have working level contact with customers and suppliers. In predictable and structured areas may supervise others. Makes decisions which may impact on the work assigned to individuals or phases of the project. May have some external contact with customers.	Performs a broad range of complex technical or professional work activities, in a variety of contexts.	-understands and uses appropriate methods, tools and applications - demonstrates an analytical and systematic approach to problem solving - takes the initiative in identifying and negotiating appropriate development opportunities - demonstrates effective communication skills - contributes fully to the work of teams, plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation and procedures - absorbs and applies technical information - works to required standards - understand and uses appropriate methods, tools and applications - appreciates the wider field of information systems, and how own role relates to other roles and to the business of the employer

4	**Enable**	Works under general direction within a clear framework of accountability. Exercises substantial personal responsibility and autonomy. Plans own work to meet given objectives and processes.	Influences team and specialist peers internally. Influence customers at account level and suppliers. Has some responsibility for the work of others and for the allocation of resource. Participates in external activities related to own specialism. Makes decisions which influence the success of projects and team objectives.	Performs a broad range of complex technical or professional work activities, in a variety of contexts.	- selects appropriately from applicable standards, methods, tools and applications - demonstrates an analytical and systematic approach to problem solving - communicates fluently orally and writing and can present complex technical information to both technical and non-technical audiences - facilitates collaboration between stakeholders who share common objectives plans, schedules and monitors work to meet time and quality targets and in accordance with the relevant legislation and procedures - rapidly absorbs new technical information and applies it effectively - has a good appreciation of the wider field of information systems, their use and how they relate to the business activities of the employer of client - maintains an awareness of developing technologies and their application and takes some responsibility for personal development

	5	**Ensue/Advise**	Works under broad direction. Is fully accountable for own technical work and/or project/supervisory responsibilities. Receives assignments in the form of objectives. Establishes own milestones and team objectives, and delegates responsibilities. Work is often self- initiated.	Influences organisation, customers, suppliers and peers within industry on the contribution or won specialism. Has significant responsibility for the work of others and for the allocation of resources. Makes decisions which impact on the success of assigned projects i.e. results, deadlines and budget. Develops business relationships with customers.	Performs a challenging range and variety of complex technical or professional work activities. Undertake work which requires the application of fundamental principals in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer or organisational requirements.	- advises on the available standards, methods, tools and applications relevant to won specialism and can make correct choices from alternatives - analyses, diagnoses, designs, plans, executes and evaluates work to time, cost and quality targets - communicates effectively, formally and informally, with colleagues, subordinates and customers -demonstrates leadership - facilitates collaboration between stakeholders who have diverse objectives - understands the relevance of own areas of responsibility or specialism to the employing organisation - takes customer requirements into account when making proposals - takes initiative to keep skills up to date - mentors more junior colleagues - maintains and awareness of developments in the industry - analyses requirements and advises on scope and options for operational improvement - demonstrates creativity and innovation in applying solutions for the benefit of the customer

	6	**Initiate/Influence**	Has defined responsibility for a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and delegates responsibilities. Is accountable for actions and decisions taken by self and subordinates.	Influences policy formation on the contribution of own specialism to business objectives. Influences a significant part of own organisation and influences customers and suppliers and industry at senior management level. Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance. Develops high-level relationships with customers, suppliers and industry leaders.	Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the formulation of IT strategy. Creatively applies a wide range of technical and/or management principles.	- absorbs complex technical information and communicates effectively at all levels to both technical and non-technical audiences - assesses and understands risk - understands the implications of new technologies - demonstrates clear leadership and the ability to influence and persuade - has a broad understanding of all aspects of IT and deep understanding of own specialism - understand and communicates the role and impact of IT in the employing organisation and promotes compliance with relevant legislation - takes the initiative to keep both own and subordinates skills up to date and to maintain an awareness of developments in the IT industry
	7	**Set Strategy/Inspire**	Has authority and responsibility for all aspects of a significant area of work, including policy formation and application. Is fully accountable for actions taken and decisions made both by self and subordinates.	Makes decisions critical to organisational success. Influences developments within the IT industry at the highest levels. Advances the knowledge and/or exploitation of IT within one or more organisations. Develops long-term strategic relationships with customers and industry leaders.	Leads on the formulation and application of strategy. Applies the highest level of management sand leadership skills. Has a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment.	- has a full range of strategic management and leadership skills - understand, explains and presents complex technical and non-technical audiences at al levels up to the highest in a persuasive and convincing manner - has a broad and deep IT knowledge of the activities and those businesses and other organisations that use and exploit IT - communicates the potential impact of emerging technologies on organisations and individuals and analyses the risks of using or not using such technologies - assesses the impact of legislation, and actively promotes compliance - takes the initiative to keep both own and subordinate's skills up to date and to maintain and awareness of developments in IT in own area(s) of expertise

Schedule 2 – Invoicing

Invoicing Schedule

Implementation Costs

Following award the supplier shall create and agree
with HMCTS
- a finalised implementation plan (that shall not significantly be different from their proposal) detailing all key milestones, activity, timescales, roles and responsibilities required to deliver the implementation; and
- acceptance criteria for each key milestone (discovery, design, build, test, implement)

Invoices shall be issued on completion of each milestone upon receiving written confirmation from HMCTS that the milestone has been achieved

Should the final milestone payment account for less than 20% of the overall implementation cost this shall be merged with the cost of the previous stages until the 20% threshold is achieved, and then invoiced on completion of all the merged stages.

reserve the right

BAU Costs

As part of the implementation the supplier shall agree with HMCTS the roll out profile of the scheme in terms of HMCTS users and the (likely) number of scheme members.

The monthly costs provided in the TCO tab shall be applied to that profile to determine the monthly costs until full roll out is achieved, at which point the monthly costs become fixed until further scheme growth is achieved.

Invoice frequency shall be agreed with the successful supplier

PUAS Financial Performance Controls

	Implementation	**Delay Payments**
1		Further to contract award (and no less than 2 weeks following the contract kick-off meeting) the successful supplier shall create and agree with HMCTS an implementation plan which shall include key milestone dates (and associated deliverables/acceptance criteria).
2		If a key milestone is not been achieved the supplier shall apply a delay payment in respect the charges for that key milestone.
3		Delay payments shall accrue at a daily rate of £500, with any part day's delay counting as a day.
4		The duration of each delay shall be calculated from the relevant key milestone date to (and including) the latter of: - the date on which the key milestone is achieved - a period of 30 days commencing from the date the milestone should have been achieved
5		The Parties agree that Delay Payments are required to protect a legitimate business interest and are not extravagant, exorbitant or unconscionable.
6		Delay payments are exclusive of VAT.
7		Where a period of delay is directly attributable to HMCTS the direct resulting delay shall not incur any delay payment.
8		Delay payments shall be deducted from the supplier's invoice for that milestone.
9		Should any changes be agreed by both parties to the implementation plan key milestone dates these, and each party's explicit agreement, must be captured in writing (e-mail is acceptable). These amended dates shall then form the basis for calculating any subsequent delay but shall not affect any retrospective delay.
10		Should the supplier miss one or more interim milestones but still achieve the overall implementation completion date (including all associated deliverables in line with the acceptance criteria), they shall be entitled to invoice for all previous delay payment deductions.

BAU	**Service Credits**
1	The 'KPIs' tab in the sets out how performance will be measured and the Service Points that apply.
2	The supplier shall monitor its performance against each KPI and provide a monthly report detailing the level of service actually achieved.
3	If in any month a KPI failure occurs, Service Credits shall be deducted from the charges for the following month. If any specific KPIs refer to both service availability and system response times, the system response times achieved by the supplier for any period of time during a month during which the relevant Service or element of a service is determined to be non-available shall not be taken into account in
4	calculating the average system response times over the course of that month. Accordingly, the supplier shall not incur any Service Points for failure to meet System Response Times in circumstances where such failure is a result of, and the Supplier has already incurred Service Points for, the Service being Non-Available.
5	Service credits shall be annually capped to 15% of the charges paid and/or are due to be paid in the period of either a) the 12 months from scheme go-live or b) in the period of 12 months immediately preceding the month in respect of which the service credits have accrued.
6	The total Service Credits applicable for that month shall be calculated in accordance with the following formula: SC = TSP x Z x AC Where: - SC is the total Service Credits for that month - TSP is the total Service Points that have accrued for that month - Z is 1% (percentage deduction per service point) - AC is the total charges payable for that month
7	Any changes to these charges shall be developed and agreed by both parties following the change control process

Part B - Terms and conditions

1. Call-Off Contract start date and length

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

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

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

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

5. Due diligence

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

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

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

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

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

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

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

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

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

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

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

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

14. Standards and quality

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

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

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

Code of Practice.

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

17. Guarantee

17.1 Not required

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

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

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

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

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and

8.87 to 8.88 (Waiver and cumulative remedies)

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

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

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

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

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

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

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

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

22. Handover to replacement supplier

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

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

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

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

23. Force majeure

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

consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

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

25. Premises

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

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

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

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

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

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

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

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

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

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

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

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

Not used

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7

Schedule 3 - Collaboration agreement

Not used

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

- "Agreement" means this collaboration agreement, containing the Clauses and Schedules
- "Call-Off Contract" means each contract that is let by the Buyer to one of the Collaboration Suppliers
- "Contractor's Confidential Information" has the meaning set out in the Call-Off Contracts
- "Confidential Information" means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information

- "Collaboration Activities" means the activities set out in this Agreement
- "Buyer Confidential Information" has the meaning set out in the Call-Off Contract
- "Default" means any breach of the obligations of any Collaboration Supplier or any default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties
- "Detailed Collaboration Plan" has the meaning given in clause 3.2
- "Dispute Resolution Process" means the process described in clause 9
- "Effective Date" means 15th June 2020
- "Force Majeure Event" has the meaning given in clause 11.1.1
- "Mediator" has the meaning given to it in clause 9.3.1
- "Outline Collaboration Plan" has the meaning given to it in clause 3.1
- "Term" has the meaning given to it in clause 2.1
- "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the "Term").

2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

Not used

4. Collaboration activities

Not used

5. Invoicing

5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.

5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

6.2 Each Collaboration Supplier warrants that:

6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party

6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors

6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise

6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:

6.3.1 or becomes public knowledge other than by breach of this clause 6

6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party

6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure

6.3.4 independently developed without access to the Confidential Information

6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction

6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

7.1 Each Collaboration Supplier warrant and represent that:

7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£ ,000)].

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage

8.5.2 special loss or damage

8.5.3 consequential loss or damage

8.5.4 loss of profits (whether direct or indirect)

8.5.5 loss of turnover (whether direct or indirect)

8.5.6 loss of business opportunities (whether direct or indirect)

8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.

9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.

9.3 The process for mediation and consequential provisions for mediation are:

9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the Chairman of the Law Society to appoint a Mediator

9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations

9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings

9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives

9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non-binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will

continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire

agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

11.5.1 Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

Schedule 4 - Alternative clauses

NOT USED

Schedule 5 – Guarantee

NOT USED

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.11 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-

	card--2.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start

	Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working

	for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security Management Plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.

Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

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

Annex 1 - Processing Personal Data

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

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: The Bar Council on behalf of HMCTS will determine the data that will be used to pass onto the supplier to process.
Duration of the Processing	The duration will be up to four years from the contract start date
Nature and purposes of the Processing	For the 'Smart Card' to be issued, Legal Professionals will register through an independent body such as the Bar Council & become accredited users once approved.
Type of Personal Data	Legal professional names, professional title, location
Categories of Data Subject	Legal Professionals
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	The system the supplier will use shall be capable of storing all the associated data for a 12-month period

2. Undertakings of Both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every 6 months on:

(i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex.

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(i) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3**. Data Protection Breach**

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4**. Audit**

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

(c)

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit

(b) and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(c) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these

Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(d) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

9. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 18.5 (*Ending the contract*).

10. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

11. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.