



G-Cloud 12 Call-Off Contract

Prj_7609 con_19658 - PTTP EUCS Contract 2021 V1.0 Final

Part A: Order Form	2
Schedule 1: Services	12
Schedule 2: Call-Off Contract charges	12
Part B: Terms and conditions	13
Schedule 3: Collaboration agreement	32
Schedule 4: Alternative clauses	44
Schedule 5: Guarantee	49
Schedule 6: Glossary and interpretations	57
Schedule 7: GDPR Information	68

Part A: Order Form

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

Digital Marketplace service ID number	https://www.digitalmarketplace.service.gov.uk/g-cloud/services/965211947051475 965211947051475
Call-Off Contract reference	con_19658
Call-Off Contract title	PTTP EUCS Contract 2021
Call-Off Contract description	Transformation advice and delivery to implement end user compute (EUC) cloud services, subject to statements of work.
Start date	1 st November 2021

Expiry date	31 st October 2022
Call-Off Contract value	<p>Capped at £1,160,000 subject to values agreed in Statements of Work.</p> <p>[REDACTED]</p> <p>For the avoidance of doubt, this Order Form does not commit the Buyer to spend any amount greater than the minimum value.</p>
Charging method	<p>The preferred charging method shall be fixed price per for agreed deliverables completed each month (as defined in statements of work)</p> <p>The parties may from time to time, subject to Statements of Work, enter into SOWs on a SFIA rate-based services no longer than 10 days' duration each (or as otherwise authorised by the Buyer), for the purpose of defining scope of and Charges for new or materially changed Deliverables.</p>
Purchase order number	Please refer to purchase order (to follow)

From the Buyer	Secretary of State for Justice 10 South Colonnade London E14 4PR
To the Supplier	Content and Cloud Ltd Fountain House, 130 Fenchurch Street, London, England, EC3M 5DJ Company number 07949424
Together the 'Parties'	

Principal contact details

For the Buyer: [REDACTED]

For the Supplier: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract shall commence on the start date specified above
Ending (termination)	<p>This Call-Off Contract shall expire 12 months following the start date, subject to any extension in accordance with the extension period provisions below.</p> <p>The length of notice required in respect of Clause 18.6 shall be no less than 90 Working Days.</p> <p>For the avoidance of doubt, the Buyer's rights of termination in respect of clause 18.1 shall apply unamended.</p>
Extension period	<p>The Buyer shall have the right to extend this Call-Off Contract for 2 (two) periods of up to 6 months, by giving the Supplier 30 days' written notice. Such extension periods shall be subject to clauses 1.3 and 1.4. of the Framework Agreement.</p> <p>Extensions which extend the Term beyond 24 months in total are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. of the Framework Agreement.</p> <p>The extension period shall not exceed the maximum permitted under the Framework Agreement which is 24 months.</p>

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	<p>This Call-Off Contract is for the provision of Services under:</p> <ul style="list-style-type: none">• Lot 3: Cloud support
--------------------	--

G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:
Additional Services	As described in Schedule 1
Location	The Services will be delivered remotely to HMPPS sites and specifically, to 3rd Floor 10 South Colonnade, Canary Wharf, E14 4PU
Quality standards	<p>The Supplier shall ensure that the Supplier staff shall at all times during the Call Off Contract Period:</p> <ul style="list-style-type: none"> - be appropriately experienced, qualified and trained to supply the Services in accordance with this Call Off Contract; - apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Services. - have undergone a pre-employment check to the standard of HMG Baseline Personnel Security Standard (BPSS) or equivalent. <p>The Supplier shall also ensure the Subcontractors and the Supplier staff with access to system configuration, system code, and cryptographic key material, or directly handling (e.g. transporting) large volumes of security classified data (or as directed to do so by Buyer Security governance), shall be cleared to SC (Security Check) level at a minimum.</p> <p>Acceptance Criteria:</p> <ul style="list-style-type: none"> - Supplier shall propose Deliverable Acceptance criteria for each Deliverable in each SOW. - Buyer shall review and either confirm or reasonably revise the proposed acceptance criteria (such confirmation or review not to be unreasonably withheld or delayed) - Supplier shall record the confirmed and/or revised acceptance criteria (the 'Acceptance Criteria'), or such Acceptance Criteria shall be specified within the Statement(s) or Work. - In the event that Acceptance Criteria have not been confirmed in accordance with the above three steps, relevant measurable requirements specified in Schedule 1 shall be construed as Acceptance Criteria.

Technical standards:	The technical standards used as a requirement for this Call-Off Contract shall be as specified in Statement(s) of Work and Schedule 1 (Services).
Service level agreement:	<p>Supplier shall utilise appropriately qualified Supplier staff and retains ownership of both Capacity Management and responsibility for the quality of service which at a minimum will be delivered to ISO 9001 / ISO 27001 standards and the Government Digital Services guidance.</p> <p>In the event that any Deliverable does not meet the relevant Acceptance Criteria, Supplier shall within two days of notification by Buyer, submit a remedial action plan to Buyer and the Parties shall meet to agree remedial actions in good faith.</p> <p>Following completion of the relevant remedial actions or within 10 days of the Buyer's notification of the relevant Deliverable failing to meet the Acceptance Criteria (whichever is sooner), the Buyer may either request further remedial action or will follow the Variation process to remove the relevant Deliverable (or partial Deliverable) from scope and amend the Charges in accordance with the relevant Variation impact assessment.</p>
Onboarding	Supplier shall cooperate with Buyer's reasonably required onboarding activities
Offboarding	<p>Supplier shall build knowledge transfer (KT) into all activities and Deliverables, including KT to Buyer's exit and transition management resources (and other third parties where relevant).</p> <p>The Supplier shall provide all documentation and artefacts developed and deliverable to the Buyer during the call-off contract duration.</p>
Collaboration agreement	<p>Supplier shall make reasonable adjustments to synchronise their delivery of products and outcomes with Buyer's third party service providers to the PTTP and shall in any case reasonably align outputs with those identified by the Buyer's governance processes.</p> <p>Where Deliverables are closely aligned with parallel work of other projects within the PTTP Portfolio, Buyer may request Supplier to take ownership and lead on development of such Deliverables for the PTTP</p>
Limit on Parties' liability	<p>The annual total liability of either Party for all Property defaults will not exceed five hundred thousand pounds (£500,000).</p> <p>The annual total liability for Buyer Data defaults will not exceed five hundred thousand pounds (£500,000) or 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>

	<p>The annual total liability for all other defaults will not exceed the greater of one million pounds sterling (£1,000,000) or 125% of the Charges payable by the Buyer to the Supplier during relevant calendar year of the Call-Off Contract Term (whichever is the greater).</p>
Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> • 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	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 15 consecutive days.</p> <p>For clarity Covid-related delay would not be considered <i>Force Majeure</i></p>
Audit	<p>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.</p> <p>Clauses:</p> <p>7.6 The Supplier's records and accounts will be kept until the latest of the following dates:</p> <ul style="list-style-type: none"> • 7 years after the date of Ending or expiry of this Framework Agreement • 7 years after the date of Ending or expiry of this Call-Off Contract to expire or End • Another date agreed between the Parties <p>7.7 During the timelines highlighted in clause 7.6, the Supplier will maintain:</p>

- commercial records of the Charges and costs (including Subcontractors' costs) and any variations to them, including proposed variations
- books of accounts for this Framework Agreement and all Call-Off Contracts
- MI Reports
- access to its published accounts and trading entity information
- proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Framework Agreement
- records of its delivery performance under each Call-Off Contract, including that of its Subcontractors.

7.10 The Supplier will allow the Representatives of CCS, Buyers receiving Services, the Controller and Audit General and their staff, any appointed representatives of the National Audit Office, HM Treasury, the Cabinet Office and any successors or assigns of the above access to the records, documents, and account information referred to in clause 7.7 (including at the Supplier's premises), as may be required by them, and subject to reasonable and appropriate confidentiality undertakings, to verify and review:

- the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement)
- any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call-Off Contract only
- the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier
- any other aspect of the delivery of the Services including to review compliance with any legislation
- the accuracy and completeness of any MI delivered or required by the Framework Agreement
- any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records

	<ul style="list-style-type: none"> the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date. <p>7.13 Each Party is responsible for covering all their own other costs incurred from their compliance with the Audit obligations.</p>
Buyer's responsibilities	<p>The Buyer shall be responsible for:</p> <ul style="list-style-type: none"> From commencement, providing access to a named Buyer designated point of contact with oversight of all matters relating to this assignment (the PTTP Project Manager'), including for issues escalation and resolution. During the delivery of the Services, support from and access to the Buyer's core project team and appropriate stakeholders as reasonably required for development of the related Deliverables. Sign-off of Deliverables by the Buyer subject to the Acceptance Criteria (as defined in the Quality Standards section of this Contract) Appropriate participation in meetings, interviews and workshops scheduled in accordance with the working practices agreed with the PTTP Project Manager, to contribute to the synchronisation and completion of the Deliverables and provision of necessary Dependencies required to complete the deliverables.. Ensuring the availability of appropriate representatives from the Buyer's suppliers (e.g. ATOS) for such workshops and meetings, as and when reasonably required by the Supplier; Making introductions with Buyer's representatives and with suppliers when needed, including explaining the Supplier's role and the purpose of this engagement to the relevant their representatives, and for securing their input and attendance at meetings, workshops and interviews; The timely provision to the Supplier of (a) all identified and requested relevant information and materials; and (b) relevant documentation taking account of any information security requirements to enable secure and swift access to relevant information; Completeness and accuracy of information provided by Buyer to Supplier. (For the avoidance of doubt, audit, test or verification of information will be out of scope of the Services unless otherwise expressly agreed.) Decision making/approvals when required as dependency on Deliverables; Notwithstanding the Supplier's responsibility for making recommendations, final procurement and other management decisions will be the responsibility of the Buyer; Access to Buyer's premises if required; To notify Supplier promptly if Buyer becomes aware of any material inaccuracy of the information or data you have provided or if any of requirements change or if Buyer becomes aware of any

	<p>conflict or ambiguity in respect of the agreed requirements or any circumstances or events which may impact the provision of the Services within the anticipated timescales;</p> <ul style="list-style-type: none"> • To maintain a permanent back up of all data provided to Supplier; • To seek appropriate advice on matters outside Supplier's scope (e.g. legal advice); • To provide relevant existing documentation at the start of the project and data from systems (e.g. ServiceNow, CMDB) within 10 days, • Review and approval of any suitable replacement Supplier staff proposed by Supplier. For the avoidance of doubt, the Supplier's preferred team shall be available to begin work from the start of the Contract. • Where Buyer needs to share work-in-progress information from Supplier, including any extracts, with third parties please check with us first so that we can check that any extracts are not misleading and that any necessary disclaimers are in place. • Buyer will not rely on any drafts or oral comments or advice unless the relevant content has been finalised as a Deliverable (or partial Deliverable, as the case may be).
Buyer's equipment	<p>The Buyer's equipment to be used with this Call-Off Contract includes configured End User Devices issued by the Buyer and compliant with the Buyer's security requirements.</p>

Supplier's information

Subcontractors or partners	<p>Supplier will on occasions use Subcontractors. All Subcontractors will be recruited by Supplier and utilised in accordance with this schedule. If Supplier does use a Subcontractor that accounts for 20% or more of the Charges for the relevant SOW, it must notify Buyer including the Subcontractor's identifying details.</p>
-----------------------------------	---

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	<p>The payment method for this Call-Off Contract is BACS</p>
-----------------------	--

Payment profile	The payment profile for this Call-Off Contract shall be invoice to be paid on completion of work / monthly in arrears.
Invoice details	The Supplier will issue electronic invoices monthly. 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 Email: [REDACTED]
Invoice information required	All invoices must include Purchase Order or Project Reference and deliverables.
Invoice frequency	Invoices to be sent monthly/ subject to Services purchased.
Call-Off Contract value	Subject to Statements of Work, the total value of this Call-Off Contract is capped at £1,160,000 (excluding VAT)
Call-Off Contract charges	See schedule 2 for a full breakdown

Additional Buyer terms

Performance of the Service and Deliverables	See Schedule 1 Service of this Order form.
Guarantee	Not used
Warranties, representations	Not used
Supplemental requirements in addition to the Call-Off terms	Not Used

Alternative clauses	Not used
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not used
Public Services Network (PSN)	Not Used
Personal Data and Data Subjects	Refer to Schedule 7, 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 (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	[REDACTED]	[REDACTED]
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]

Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Schedule 1: Services

- 1.1 The Supplier shall deliver the Services as detailed in their G Cloud Service offer.
- 1.2 SOW001 as agreed in the Annex to this Schedule 1 will form the basis for all further SOWs over the duration of this contract
- 1.3 Each SOW will align as much as is feasible to the Programme Increment PI structure of the Programme Delivery plan as advised by the Buyer during SOW agreement.
- 1.4 SOW001 will include those services Delivered from 1st November 2021 to 14th January 2022 (less any planned hiatus between PIs or due to agreed contractor hiatus) with subsequent SOWs being no less than 4 weeks and no more than 8 weeks in duration.
- 1.5 The Acceptance Criteria in each SOW must be met or otherwise agreed through the Acceptance Criteria process: This is the agreed Authority to Proceed and is a pre-requisite to any additional SOW.
- 1.6 SOWs may run in parallel or overlap in duration as agreed to accommodate new work and will include the drafting and presentation for agreement of the subsequent / follow-on SOW as a Deliverable.

1.2 Activities and Deliverables

The activities and Deliverables shall be in accordance with the Suppliers Service Offer and as further specified in statements of work from time to time, including the Deliverables and the activities set out in the table below:

Proposal includes delivery of the defined outputs:

APPS-003	Continued technical delivery of automated application delivery and deployment
MMD-001	Technical delivery on MMD Policy and EUC Optimisation
AVD-003	Continued technical delivery of Azure Virtual desktop
VICD-003	Delivery of enhanced Application Life Cycle management controls enabling EUC environment and application management - VICTOR
ASC-001	Delivery of enhanced EUC application controls deployed across MoJO EUC estate.

This will include appropriate ownership and implementation of changes, as well as synchronising outputs and dependencies with other partners as required. This will include but is not limited to, Atos, DXC and other PTPP delivery partners

The Supplier will

- o own the technical outcomes.
- o provide and manage the capacity to deliver agreed outcomes from PTPP projects
 - Dependency: Input from Programme on priority of delivery via PTPP Project Manager
 - Outcome: The Supplier has the appropriate level of cost-effectiveness at all times

- o Provide a Project Manager (PM) function that enable the reduction of Architectural support
 - Outcome: reduction in cost, increase in Supplier effectiveness
- o The Supplier PM will be the single point of contact responsible for deposition and alignment of Supplier resources to key project activities and Deliverables
- o All Buyer inputs and Dependencies will be routed via the PM who will act as the single point of contact for all queries & escalations.
- o Any change/addition to the scope of this SoW will be done via a change control process.
- o Dedicate at least one senior technical resource to each epic who will own issue resolutions during the defect rectification and remediation period
- o Develop, maintain and Deliver a biweekly report providing synchronisation information and progress against delivery to the PTTP Project Manager and to inform Dependencies
 - Outcome: Deliver a monthly schedule reporting on Supplier Capacity against outstanding Deliverables including forward planning information

Out of Scope

- Provision and supply of hardware and devices
- The physical rollout of devices to end-users
- The ongoing support of the PTTP implemented solutions
- Any remediation and rectification of defects after the completion of one sprint from production release date
- LLD documentation
- ASC-001: Global Protect - Any future version deployments after the current latest version deployment
- APPS-003: Packaging applications not supported on Windows 10
- Backlog Definition and Scrum management
- Measure tech Ops capabilities as part of the handover Backlog definition & management, prioritising activities, project timeframes and overarching PTTP programme outcomes remains the responsibility of the Buyer (PTTP).

Schedule 1: SOW 1 to Cover remainder of PI-11

(Frontispiece as in Contract)

Prj_7609 con_19658 - PTTP EUCS Contract 2021 SOW001

Start Date: 1st November 2021

End Date: 14th January 2022

Agreed Date (As contract)

The following Statement of Work (SOW) draws down services as described in the contract above and the services described will be delivered according to the terms and conditions of service of that contract. It is agreed that this SOW does not modify the scope or materially change the terms and conditions of service of the related contract and that any such change may only take place through the formal Variation (CCN) process.

Any “pending” work across multiple SOWs may be carried over to subsequent PIs / SOWs by Agreement. The Supplier must provide the Buyer with evidence of progress to completion with any request for partial Acceptance, Authority to proceed and in advance of payment against work in progress. An Administrative Deliverables: the Supplier will review, plan and cost each SOW within 5 working days of receipt, on the understanding that the necessary dependencies are provided by the Buyer no less than 10 working days before the end of the existing SOW it replaces.

Payment Milestones

Those deliverables marked as “completed” in the PI SOW Foundation list as of the date of contract signature are agreed as viable for invoicing immediately on contract signature.

Otherwise: The Supplier will invoice monthly (at the end of the Month) against those aspects that have completed their Acceptance Criteria and which has been agreed as completed through the Acceptance Criteria process over the previous month. Dispute over Acceptance over a particular item shall not unreasonably delay payment against undisputed deliverables.

Where Outcomes are initially defined for a 20% reserve for ad hoc work and marked as Completed, this is fit for payment. In all SOWs from SOW002 this “pool” will be suitable for a defined and agreed volume of work within a range . Additional KPIS and performance measures will be required and agreed for each SOW by the Supplier and reported the Buyer to monitor the demand . Where the agreed volume is exceeded by +10% or more the supplier may request a change to the SOW or the subsequent SOW to reflect the additional capacity required.

[REDACTED]

Programme Increment (PI) SOW Foundation (updated for Each SOW)

<i>EPIC / WORKSTREAM</i>	<i>OUTCOME & DESCRIPTION</i>	<i>ACCEPTANCE CRITERIA</i>	<i>RAID/ Out of Scope</i>	<i>DATE (month end un- less specified)</i>
AVD-003: Azure Virtual Desktop Delivery				
Azure Virtual Desk- top Delivery	AVD Use Case 2 Design	AVD Use Case 2 Design Drafted & Approved at TDA		Nov-21
	AVD Use Case 2 Technical Development	AVD Use Case 2 development complete and SIT ticket created.	Assumption: AVD Infrastructure is using existing Nerdio infrastructure AD services are available Dependencies: Dependency on Atos with service accounts Dependency on Azure LZ networks Out of Scope: We will be cloning the policies that are a	Dec-21

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	RAID/ Out of Scope	DATE (month end un- less specified)
			already available on the windows 10 laptops and desktops. Additional configuration policies are out of scope	
	AVD Use Case 2 Technical Development			
	AVD Use Case 2 User testing	AVD Use Case 2 UAT complete (technical support to UAT)	Dependency: UAT Test plan Out of Scope: Fixing issues which are a result of a new requirement(s)	Dec-21
	AVD Use Case 2 Defect Remediation	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	Dependency: SIT Test plan Out of Scope: Fixing issues which are a result of a new requirement(s)	Dec-21
APPS-003: Application Integration & Delivery	OUTCOME 1 - Technical assessment/design, MoJO platform Integration, test support and remediation of applications defined within the MoJ DAA Applications Road Map. This includes core Line of business applications and Secure Applications			
	Packaging and Integration of c. 30 LoB applications or weblinks	Application SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.		Dec-21

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	RAID/ Out of Scope	DATE (month end un- less specified)
	Packaging and Integration of Assistive Tech Applications (c.3)	Application SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.		Dec-21
	VISOR Tactical Design Support (Secure App)	Design Drafted & Approved at TDA (support only)		Oct-21
	VISOR Tactical technical Integration	Application SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.		Nov-21
	VISOR Tactical Defect Remediation	VISOR Defect Remediation following SIT Testing (4 week defect remediation period required after this date)		Nov-21
	PNC Design Support (Secure App)	Design Drafted & Approved at TDA (support only)		Oct-21
	PNC Tactical technical Integration	Application SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.		Oct-21
	PNC Tactical Defect Remediation	PNC Defect Remediation following SIT Testing (4 week defect remediation period required after this date)		Nov-21

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	RAID/ Out of Scope	DATE (month end unless specified)
ASC-001: Implementation of Application Security Controls	OUTCOME 1 - Technical assessment/design, MoJO platform Integration, test support and remediation of Application security controls a. 'Global Protect' deployed and operational on all live devices b. 'AppLocker' deployed and operational on all live devices			
	Packaging and Integration of Global Protect version	Global Protect SIT Testing complete		Nov-21
	Packaging and Integration of App Locker version	App Locker SIT Testing complete		Dec-21
	Global Protect and AppLocker Remediation	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.		Dec-21
	OUTCOME 2 - Publication of material and support provision to enable BAU to manage and maintain these controls 'in life', this should include : - Design Material Publication - Technical & Design Knowledge Articles - Support to Global Protect & AppLocker technical knowledge transfer	Service Acceptance of hand over material (KBA / Design documented in Wiki)		Dec-21
VICD-003: Implementation of Application Life Cycle Management Controls	OUTCOME 1 - Delivery of enhanced Application Life Cycle management controls enabling EUC environment and application management (a technology enabler to provide BAU teams with the ability to upgrade / downgrade Applications at scale in a co-ordinated / controlled manner). Deploy controls in all environments for large scale code / application management			

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	RAID/ Out of Scope	DATE (month end unless specified)
	Technical Input to Application Life Cycle Management documents (20 documents maximum)	Application Life Cycle Management Documents complete (20)		Dec-21
	VICTOR technical implementation and deployment across all environments	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.		Dec-21
	VICTOR technical Defect Remediation	VICTOR Defect Remediation following SIT Testing (4 week defect remediation period required after this date)		Dec-21
	OUTCOME 2 - Publication of material and support provision to enable BAU to manage and maintain these VICTOR in life, this should include : - Design Material Publication - Technical & Design Knowledge Articles - Support to Global Protect & AppLocker technical knowledge transfer	Service Acceptance of hand over material (KBA / Design documented in Wiki)		Dec-21
MMD-001: MMD Policy and EUC Optimisations	OUTCOME 1 : Review and technical Implementation of EUC modifications (MMD policy, EUC application packaging modification and In-tune optimisations)			
	Custom Outlook profile technical Implementation (Outlook PWA)	Outlook PoC PWA SIT Complete		Dec-21
	Core LoB app Access optimisations (CSR my detail Regional Split, CSR access methodology)	Application SIT testing complete (4 week defect remediation period required after this date)		Nov-21

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	RAID/ Out of Scope	DATE (month end un- less specified)
Product Defect Re- mediation & Prod- uct Improvements and Knowledge Transfer	OUTCOME 1: Allocation of 20% capacity to address ad hoc technical defects that require re-remediation. This capacity should also be able to be used to optimise the product set or knowledge transfer to Service support teams if required (based on technical need and user feedback). This optimisation / KT capacity will be planned on a sprint by sprint basis.			Dec-21

NB The Gap between PI11 and PI12 will be agreed through SOW002. Where SOW001 outcomes are completed the Buyer and Supplier may agree to begin or prepare for PI-12 activities where the activities and value can be agreed in writing in advance of SOW002 and to be included therein.

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	DATE (month end unless specified)	Agreed STATUS
Pi12 (05th January > 02nd March)				
Azure Virtual Desk- top Site Integra- tion (Use Case 2 & 3)	OUTCOME 1 - Delivery of AVD solution to meet AVD Use case 2 (Provision of the 'Mojo shared desktop MMD' experience via an Azure virtualised desktop capability to support the operation of a newly built prison (FiveWells).			Pi12
	AVD Use Case 2 Technical Site Implementa- tion	SIT testing complete (4 week de- fect remediation period required after this date). Test lead declared SIT ticket closed.	Jan-22	Pi12
	AVD Use Case 2 Technical Site Defect Re- mediation	VICTOR Defect Remediation fol- lowing SIT Testing (4 week defect remediation period required after this date)	Feb-22	Pi12
	AVD Use Case 3 Technical Design (Use case 2 Modification)	AVD Use Case 3 Design Drafted & Approved at TDA	March 02 2022	Pi12

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	DATE (month end unless specified)	Agreed STATUS
	AVD Use Case 3 Technical Development	AVD Use Case3	TBC	Pi12
	AVD Use Case 3 Technical Implementation(Use case 2 Modification)	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	Jan-22	Pi12
	OUTCOME 2 - Publication of material and support provision to enable BAU to manage and maintain the AVD solution 'in life', this should include but is not limited to the following: - Design Material Publication - Technical & Design Knowledge Articles - 2 (1 hour) KT sessions with service	Service Acceptance of hand over material (KBA / Design documented in Wiki)	March 02 2022	Pi12
Application Design, Integration & Delivery	OUTCOME 1 - Technical assessment/design, MoJO platform Integration, test support and remediation of applications defined within the MoJ DAA Applications Road Map. This includes core Line of business applications and Secure Applications			Pi12
	Packaging and Integration of c. 20 LoB applications or weblinks (group 6)	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	March 02 2022	Pi12
	Packaging and Integration of Assistive Tech Applications (c.5) (group 6)	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	March 02 2022	Pi12
	Mercury Technical Design (Including Options Assessment - continuation of existing design)	Options assessed Design Drafted & Approved at TDA (support only)	Jan-22	Pi12

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	DATE (month end unless specified)	Agreed STATUS
	Mercury Technical Implementation (post Options Assessment)	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	Feb-22	Pi12
	Mercury Tactical Defect Remediation	Defect Remediation following SIT Testing (4 week defect remediation period required after this date)	Mar-22	Pi12
	VISOR Strategic Design Production (Secure App) inc Options assessment	Design Drafted & Approved at TDA (support only)	Feb-22	Pi12
	VISOR Strategic Technical Implementation (post Options Assessment)	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	March 02 2022	Pi12
	VISOR Strategic Defect Remediation	Defect Remediation following SIT Testing (4 week defect remediation period required after this date)	March 02 2022	Pi12
Code Pipeline Control (VICTOR)	OUTCOME 1 - Complete deployment of VICTOR across all MoJO environments and define VICTOR backlog for BAU hand over			Pi12
	Review current VICTOR implementation and define scope to get to VICTOR complete (Deployed across all environments and optimised for mass roll out)	Scope Approved at TDA	Jan-22	Pi12
	Define VICTOR back log (inc ITHC remediation required)	N/A	N/A	Pi12
	Implementation of VICTOR Back Log	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	March 02 2022	Pi12

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	DATE (month end unless specified)	Agreed STATUS
	Publication of material and support provision to enable BAU to manage and maintain the VICTOR solution 'in life', this should include but is not limited to the following: - Design Material Publication - Technical & Design Knowledge Articles - 2 (1 hour) KT sessions with service	Service Acceptance of hand over material (KBA / Design documented in Wiki)	March 02 2022	Pi12
Pool Laptop Integration	OUTCOME 1: Technical implementation (working with MS & MoJO) to implement existing MMD policies on shared desktop and pool Laptops. Technical support required to ensure the MMD policies are appropriate for the device. Custom policy application may be required for SOCT laptops.	To be agreed at start of Pi	March 02 2022	Pi12
SOCT Laptop Integration	OUTCOME 1: Technical implementation (working with MS & MoJO) to implement existing MMD policies SOCT Laptops. Technical support required to ensure the MMD policies are appropriate for the device. Custom policy application may be required for SOCT laptops.	To be agreed at start of Pi	March 02 2022	Pi12
MMD Policy and EUC Optimisations	OUTCOME 1 : Review and technical Implementation of EUC modifications (MMD policy, EUC application packaging modification and In-tune optimisations)			Pi12
	Technical implementation of User centred MDE USB policy (modified from device centric policy) this will involve working with Microsoft and MoJ to implement a tactical (SIDS) and a strategic (policy) solution.	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	Feb-22	Pi12
	Assess position and modify Dell Command Update / BIOS approach if required.	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	Jan-02	Pi12

EPIC / WORKSTREAM	OUTCOME & DESCRIPTION	ACCEPTANCE CRITERIA	DATE (month end unless specified)	Agreed STATUS
	Outlook PWA implemented across MoJO estate	SIT testing complete (4 week defect remediation period required after this date). Test lead declared SIT ticket closed.	Feb-22	Pi12
	OUTCOME 2 - Publication of material and support provision to enable BAU to manage and maintain the shared desktop optimisations 'in life', this should include but is not limited to the following: - Design Material Publication - Technical & Design Knowledge Articles - 2 (1 hour) KT sessions with service	Service Acceptance of hand over material (KBA / Design documented in Wiki)	March 02 2022	Pi12
Product Defect Remediation & Improvements	OUTCOME 1: Allocation of 20% capacity to address ad hoc technical defects that require remediation. This capacity should also be able to be used to optimise the product set or knowledge transfer to Service support teams if required (based on technical need and user feedback). This optimisation / KT capacity will be planned on a sprint by sprint basis.		March 02 2022	Pi12

Schedule 2: Call-Off Contract charges

2.1 Call-Off Contract Charges

Contract value is capped at £1,160,000

For each individual Statement of Work, the applicable Call-Off Contract Charges (in accordance with the charging method in the Order Form) will be fixed price calculated using the agreed relevant rates for Supplier SFIA Rates which are exclusive of any applicable expenses and exclusive of VAT.

2.2 Invoice Arrangements

Invoice payments related to those deliverables that have met their Acceptance Criteria shall be as specified in Statements of Work

Any work for which a proportion fails to meet the Acceptance Criteria in a specified period will not be accepted by the Buyer and will be completed at the Supplier's expense. The Charges applied to that proportion of work will be excluded from the total Charges due for that period. Those Charges so excluded may only be charged once the quality and standard of the work for that period has been accepted by the Buyer.

The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges.

At the beginning of each month, a review of key tasks will be agreed between the designated Supplier Point of Contact and the PTTP Project Manager as part of the monthly project delivery plan provided by the Supplier to the Buyer. PTTP Commercial will be the escalation points for the Supplier including any final sign off.

The high-level Deliverable Table above lists the anticipated areas of focus over the PI delivery plan, which will form the basis of the monthly reviews.

The Parties may agree ad hoc services via email confirmation, in which case the Parties shall amend and update the relevant Statement of Work in respect of such ad hoc services. Such ad hoc services will not require a Variation.

2.4 Supplier's Rate Card

If agreed in writing, additional services will be charged at the rate card as provided in the Supplier's published GCloud SFIA Rates.

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 18 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 6 months.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

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

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

- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

- 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
 - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
 - 5.1.4 have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

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

- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
 - 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
 - 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
 - 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
 - 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
 - 9.4.1 a broker's verification of insurance
 - 9.4.2 receipts for the insurance premium
 - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
 - 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

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

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

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

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

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

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

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

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

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

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

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

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

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

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

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

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

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

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

11.7.3 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

- 12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
- 12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- 12.2.4 providing the Buyer with any information requested by the Data Subject
- 12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

- 13.1 The Supplier must not remove any proprietary notices in the Buyer Data.
- 13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
- 13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
- 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
 - 13.6.1 the principles in the Security Policy Framework:
<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:
<https://www.gov.uk/government/publications/government-security-classifications>
 - 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:
<https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets:
<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
 - 13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance:
<https://www.ncsc.gov.uk/collection/risk-management-collection>

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

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

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
 - 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
 - 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

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

- 19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- 19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- 19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- 19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- 19.5.5 work with the Buyer on any ongoing work
- 19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
- 19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
- 19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

- 20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.
 - Manner of delivery: email
 - Deemed time of delivery: 9am on the first Working Day after sending
 - Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message
- 20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
 - 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
 - 21.6.2 there will be no adverse impact on service continuity
 - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
 - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
 - 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

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

22. Handover to replacement supplier

- 22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
 - 22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
 - 22.1.2 other information reasonably requested by the Buyer
- 22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.
- 22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

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

24. Liability

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

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

25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
 - 25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises
 - 25.5.2 comply with Buyer requirements for the conduct of personnel
 - 25.5.3 comply with any health and safety measures implemented by the Buyer
 - 25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
- 25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

- 26.1 The Buyer will supply MoJ issue laptops to the Supplier to provide the Services.

- 26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.
- 26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

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

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

28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
 - 29.2.2 age
 - 29.2.3 start date
 - 29.2.4 place of work
 - 29.2.5 notice period
 - 29.2.6 redundancy payment entitlement
 - 29.2.7 salary, benefits and pension entitlements
 - 29.2.8 employment status
 - 29.2.9 identity of employer
 - 29.2.10 working arrangements
 - 29.2.11 outstanding liabilities
 - 29.2.12 sickness absence

- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
 - 29.6.1 its failure to comply with the provisions of this clause
 - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 3 - Collaboration agreement

Not Used

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	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> 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 <p>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.</p>
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	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • 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 to be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.

Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • 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 <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also

	includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • 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	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • 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	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.

Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

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

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

Schedule 7: GDPR Information

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

Annex 1: Processing Personal Data

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

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

- 1.1 The contact details of the Supplier's Data Protection Officer are:
- 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.

Descriptions	Details
Identity of Controller for each Category of Personal Data	<p>Unless otherwise identified, for all categories of Personal data in respect of this Call-Off Contract, the Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that they are not Joint Controllers for the purposes of the Data Protection Legislation.</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none">• Business contact details of Supplier Personnel for which the Supplier is the Controller• Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller
Duration of the Processing	Call-Off Contract period

Nature and purposes of the Processing	<p>Nature: review and analysis and aggregated reporting, and custodianship of Buyer's physical hardware for all relevant processing.</p> <p>Purpose: analysis and reporting for production of Deliverables.</p>
Type of Personal Data	Names, contact details, roles
Categories of Data Subject	Staff; Buyer's third party supplier staff (e.g. for TUPE liability analysis)
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	Return of Buyer's hardware. For the avoidance of doubt, Supplier shall not process Buyer's data on any non-Buyer platform.

Annex 2: Joint Controller Agreement

Not used

1. Joint Controller Status and Allocation of Responsibilities

1.1 not used

2. Undertakings of both Parties

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

- (a) report to the other Party promptly by exception:
 - (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;
 - (ii) 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.

6. ICO Guidance

- 6.1 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 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;

(b) 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

(c) 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 procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing 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.

8. Not used

9. Termination

9.1 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

11.1 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.