Crown Commercial Service

G-Cloud 12 Call-Off Contract

prj_7617PTTP Delivery Partner Requirements – National Rollout DRAFT V0.2

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

Part A: Order Form

Digital Marketplace service ID number	**CDW Limited Cloud Professional Services** Service ID 226555311169903 GCloud 12
Call-Off Contract reference	prj_7617 con_20401
Call-Off Contract title	PTTP Delivery Partner Requirements – National Rollout
Call-Off Contract description	Deployment Services for Phase 3 National Rollout of the Prison Transforming Technology Programme (PTTP)
Start date	01/04/2022
Expiry date	31/03/2023
Call-Off Contract value	Up to £19,000,000 (inc VAT) including £12,850,887.00 (Net) £2,570,177.40 (VAT) £15,421,064.40 (Gross) i.e. £12.85M+VAT With approx. 7.6% contingency to account for change, additional pre-deployment configuration services and logistical expenses agreed in writing over the course of the multi-site deployment. Full summary table below.
[REDACTED]	
Charging method	BACS / Basware as appropriate
Purchase order number	TBC

From the Buyer	The Secretary of State for Justice Ministry of Justice Commercial and Contract Directorate Zone 3.19, 3rd Floor 10 South Colonnade Canary Wharf E14 4PU

To the Supplier	CDW LIMITED Company number 02465350 3rd Floor One New Change, London EC4M 9AF
Together the 'Parties'	

Principal contact details

For the Buyer: [REDACTED]

For the Supplier: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1st April 2022 and is valid for 12 months to the 31st March 2023 unless otherwise agreed or extended. (Principle delivery expected to end of December 2022) The date and number of days or months is subject to clause 1.2 in Part B below.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	Up to a total of 24 months in no more than x2 increments of *no less* than x3 months each

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: • Lot 3: Cloud support
G-Cloud services required	Service wrap for the deployment and early adoption services not covered by the End-User Hardware Agreements bought through the RM6068 Technology Products and Associated Services products Services including but not limited to: Provision of logistical and End User Engineering consultancy to the programme and ownership of the Device deployment process for the Phase 3 of the PTTP National Roll Out

	Establish initial contact and communication routes with end-users on device activation and utilisation including providing agreed levels of access to the Supplier deployment planning information and systems (enabling the Transformational Business Change Partner where appropriate) Early single-point -of contact activity in advance of handover to the Customer support structure including virtual floorwalking, problem solving and relay of provided Business Change information to end users and appropriate feedback. Additional pre-Deployment Device Engineering and configuration Services as required
Additional Services	Additional Services may be requested by the Buyer throughout the contract term through Change Control to amend existing Statements of Work or the addition of further Statements of Work, limited to: • Other services within scope of the Supplier's GCloud offer
Location	Due to the ongoing impact of the Covid-19 pandemic, the Supplier and Buyer will make appropriate use of remote working and engagement through remote collaboration tools such as Microsoft O365, Teams and Slack as appropriate. When Covid-19 policies permit a return to face-to-face collaboration, the Supplier may be asked to attend client meetings at the following primary location: **10 South Colonnade** **Canary Wharf** **London, E14**
Quality standards	The quality standards required for this Call-Off Contract are as specified in the GCloud 12 offer and: The Supplier will comply with those protocols and ways of working established by the Buyer's Prison Technology Transformation Programme where required either advised separately through the operational process or as an addendum added as an Annex to Schedule 1 • ISO 9001

Technical standards:	The technical standards required for this Call-Off Contract are: • The Supplier will deliver services in accordance with the requirements of the G-Cloud 12 Framework, including adherence to the Technology Code of Practice. • ISO 20000 • ISO 27001 • ISO 9001
Service level agreement:	Indicative Delivery Timeline(s) as detailed in Schedule 1: Services
Onboarding	The onboarding plan for this Call-Off Contract is **not required as this contract provides continuity of service from previous phases of the Deployment activity..**
Offboarding	**Not Required**
Collaboration agreement	• A specific Collaboration Agreement is not required. Clause 31 applies • The Supplier is expected to adopt the Buyer's Programme protocols, local security protocols necessary to gain access to secure areas and agreed approaches to ensure synchronisation and integration with existing Delivery teams as appropriate.
Limit on Parties' liability	• The aggregate annual total liability of either Party for all Property damage will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. • The annual total liability for Buyer Data defaults will not exceed £1million or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). • The annual total liability for all Supplier defaults will not exceed the greater of £1million or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater)

Insurance	The insurance(s) required will be: • a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £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 (and as required by Law)
Force majeure	• A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 10 consecutive days. • For the avoidance of doubt Covid-19 shall not be considered a Force Majeure Event for the purposes of this Call-Off Contract.
Audit	N/A
Buyer's responsibilities	The Buyer is responsible for: • Planning and arranging Site access , including the provision of security passes for the Supplier's personnel primary working locations, and passes or escorting at other sites where required in the delivery of services *where the Supplier's personnel have the appropriate security clearances;* • Contractual and Commercial management of the Buyer's third-party Suppliers, including escalation and timely resolution of issues impacting the Supplier's delivery; • Ensuring that those staff involved in handover and knowledge transfer are appropriately skilled and are made available to take on appropriate knowledge or activity required. • All Buyer-required software and third party licenses requirements • Appropriate internet access at Buyer locations • Providing a single point of contact for the project for operational delivery reporting and change management

	• Providing requested information necessary for Delivery planning within three working days, in particular: • Confirming Change to Deployment order, removal or addition of sites as soon as these are agreed through the Buyer's internal process, on the understanding that for notice of change provided less than 10 working days before the original deployment point, scaleable irrecoverable costs will be incurred by the Supplier and charged to the Buyer. The Supplier undertakes to minimise these costs as much as is possible. • Providing reasonable access to desks, conference call, staging areas and meeting facilities as required and available. • Facilitating direct access or through appropriate 3rd Parties to • Programme Deployment Plans and Delivery dependent Information as agreed in the Information Request Log • Stakeholders throughout the organisation for Delivery dependent Information exchange and planning • Systems where Delivery dependent Information is live, or not documented It is agreed that a delay in access to information or resources may result in a reduction in the quality or coverage of the deliverables, and a delay to the affected deliverables. The Supplier will take all reasonable steps to alert the Buyer to the potential impact of untimely provision of the above.
Buyer's equipment	The Buyer will provide Access to such Buyer systems, equipment and premises as is reasonable for the delivery of the contracted services.

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners **Change Adopt (Business Change Sub-contractor)**

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS following Supplier invoice
Payment profile	The payment profile for this Call-Off Contract is in arrears as defined in Schedule 2.
Invoice details	The Supplier will issue electronic invoices in arrears as per the payment profile included in Schedule 2. The Buyer will pay the Supplier according to the current Government policy for expediting payment of their Suppliers and no later than 30 days of receipt of a valid invoice
Who and where to send invoices to	Invoices will be sent to: Shared services Celtic Springs Business Park, P.O. Box 767 Newport. NP10 8FZ
Invoice information required	All invoices must include contract and PO references and be compliant with the HMRC guidance for VAT invoices.
Invoice frequency	Invoice will be sent to the Buyer in arrears as per the payment profile in Schedule 2
Call-Off Contract value	The total value of this Call-Off Contract is capped at £19M inc VAT ie. £13,859,645 +VAT The duration for the principle delivery is currently planned to end at or before 31st December 2022
Call-Off Contract charges	The breakdown of the Charges is shown within Schedule 2 of this contract Further SOWS or related Work Packages to be presented on a Fixed Price against outcomes / Deliverables basis by default. Notified Change to Deployment plans less than 10 days before the original Deployment point will incur scaleable irrecoverable costs. The Supplier under-takes to minimise these costs as much as is possible.

Additional Buyer terms

Performance of the Service and Deliverables	As described in Schedule 1
Guarantee	**N/A**
Warranties, representations	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that: • The Supplier will perform its obligations under this Call-Off Contract with all reasonable care, skill and diligence, according to Good Industry Practice. • The Supplier will not intentionally introduce disruptive elements into systems providing services to data, software or Authority Confidential Information held in electronic form. • The Supplier undertakes to the Buyer that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Call-Off Contract Order Form. • The Supplier warrants that it has full capacity and authority and all necessary authorisations, consents, licences and permissions and Intellectual Property Rights to perform this Call-Off Contract. • The Supplier represents that, in entering into this Call-Off Contract it has not committed any Fraud. • The Supplier undertakes to pay all taxes due from it to HMRC and will not indulge in "disguised employment" practices when delivering services under this Call-Off Contract, and For the avoidance of doubt, the fact that any provision within this Call-Off Contract is expressed as a warranty shall not preclude any right of termination the Buyer may have in respect of breach of that provision by the Supplier.
Supplemental requirements in addition to the Call-Off terms	**N/A**
Alternative clauses	**N/A**

Buyer specific amendments to/refinements of the Call-Off Contract terms	**N/A**
Public Services Network (PSN)	**N/A**
Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used:

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.

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

Schedule 1: Services

Original High Level Buyer Service Requirements

1. Provide a streamlined deployment experience for end users minimising end user disruption by deploying new replacement devices and peripherals.

2. Agree standard template deployment approach to a prison site and acceptable exit criteria for each site.

3. In consultation with the programme team produce

   1) a deployment plan which aligns to the Programme's priorities and delivery timeframes, and

   2) a training plan. Identifying opportunities to progress at scale and pace.

4. The Supplier is to own the provisioning, build, deployment / rollout and guide Buyer in terms of best practices, to lean the process to create efficiencies to allow for rapid rollout across the Prison estate. (from Phase 2)

Devices – MoJO devices on desks and in a good working state

5. As part of agreed deployment plans; manage device storage and logistics at site – outcome to be achieved: devices deployed to correct location and users at volumes to match asset numbers provided in deployment plans (within agreed tolerance)

6. Ensure packaging is removed with environmental consideration as priority outcome.

7. Engineer the devices deployed on site; replacing any devices DOA and ensure each device is at a "good working state" as defined by the programme – within a margin of 1% at point of user enrolment.

8. At point of deployment remove legacy PCs and follow the decommissioning approach for secure and safe disposal of assets as determined by the Programme.

9. Maintain an asset and deployment register; providing proactive management information to the programme team: frequency and methodology to be agreed with the programme

User Onboarding

10. As part of agreed deployment plan provide – Day 1 Set up for users targeted at their user role requirements. All users will be presented by the programme as "ready" to adopt their devices: volumes of users enrolled to their devices will be agreed with a margin of 1% in the deployment plan on a site by site basis (minimum set by the programme).

11. The deployment lifecycle will set the number of days of hyper/ELS for users by site: provision floor walking for users during this time – noting the security limitations of individual sites.

12. The deployment lifecycle will set the number of days of hyper/ELS for users by site: provision Re-Call service to priority users/at user's desk to reduce support calls.

13. During the deployment life cycle on site, capture and raise repeat issues with the service improvement team to inform the ongoing deployment planning and product development

14. The deployment lifecycle will set the number of days of hyper/ELS for users by site: where the deployment partner cannot resolve an incident: provide support to user to raise incidents to the Service Desk during this time and if appropriate raise incidents on behalf of users.

15. Programme will agree criteria for site Exit from hyper/ELS with the Supplier across all sites with local tolerances agreed.

Training and Business Change Adoption

16. Provide an effective change adoption experience for end users matched to the requirements of their role. Aim: to empower users to get the most from the technology, enabling improved, more effective working practices

17. To plan with the programme team and the business areas to avoid business disruption for users during the transition from Quantum to "MoJO" operating systems and Devices

18. Prior to Device Deployment and User Enrolment at a site - prepare users for the transition, making them feel comfortable with the change, understanding what changes will occur and how they will be supported through the process leaving a legacy of contribution towards lasting and sustainable change in working practices

19. To deliver effective, relevant learning for users through understanding the varying roles and responsibilities within the prison service and creating specificity in the learning delivered

20. To work with the programme to look at how we can continually improve how we prepare, deploy, train and support users/teams/groups through the transition to their new IT Service.

21. Training on SharePoint Online is in scope of the requirement but not overtly specified. Any definition of such a service will be made through the formal Change Control process applicable to the contract.

Reportable Key Performance Indicators (KPIs)

- Refinements to these KPIs and further KPIs may be read into the Contract via the agreed Change Control process. Each KPI will be reported by the Supplier as part of the overarching Delivery Management Information (MI) Briefing on a weekly basis with a full cumulative Monthly report and with immediate reporting of any developing of a significant issue at the point it is identified.
- Each Site will be delivered with a standardised approach with Supplier to scale of delivery resource to take **no more than 3 calendar weeks**, including exit. This timeframe assumes delivery of all relevant Buyer obligations in a timely manner and will allow for approximately 10% of legacy devices to continue in operation until a designated point in the Deployment Plan. Where feasible and made available users of these legacy devices should be encouraged to undergo training in the first pass of each Site to maximise efficiency.

i.e.

Site Delivery	Target
Good	Delivery made in 3 weeks or less
Approaching Target	Less than 3 working days outside target
Inadequate	5 days or more outside target*
Weekly progress reporting on a Site-specific basis for each Site during delivery.	

- During each Site engagement the Supplier will provide **EITHER standardised reports OR appropriate access to a dynamic logistical planning database** reporting on progress on Engineering, Training and Business Change engagement on a Site-by-Site basis. This will include at a minimum logistical progress or shortfalls, Asset Register updates, non-standard incident reporting, reporting of non-standard environments, risks, issues, outstanding or newly

encountered Buyer or External dependencies, (and any steps taken to mitigate) and overall progress against the 3 calendar week Site Delivery target.

i.e.

MI KPI	Target
Good	Weekly information to acceptable standard
Approaching Target	Day late or agreed / available information not provided*
Inadequate	Failure of Data Quality in the Report *
An alternative source of information and reporting may be provided by Agreement	

- The Supplier will factor in and report on current progress per Site to a multi-Site **Delivery Confidence KPI** reflecting the probability of maintaining or improving the overall Deployment timetable. This should reflect the cumulative effect of any Delays (including reasons and lessons learned) and highlighting opportunities where more rapid than expected progress can potentially compress the Deployment timetable for the Sites yet to be Deployed.

i.e.

Delivery Confidence KPI	Target
Good	On deployment target or better
Approaching Target	10 days or less behind target
Inadequate	More than 10 days behind target*

- The Supplier will endeavour to minimise disruption to the Site Users and Site controllers. They will provide an opportunity for recording **User Satisfaction KPI** feedback at each Site from the end users relating to any work disruption, balanced against the benefits of the engineering and training service engagement. This **KPI** model should be scaleable to the size, user numbers, user responsibilities and complexity of the site, with any feedback factored into next-Site Lessons Learned. i.e.
    - **Direct User Feedback** – When supporting users through the process of onboarding : Trainers share information about how differing role types require support and as such the approach is adapted in the future.
    - **Key Decision Maker Feedback** – e.g. Custodial Managers meetings. Adapt how we approach the deployment based on key challenges the prison may be facing at any given time.
    - **Engineer / Trainer Feedback** – The team have daily meetings and find iterative micro improvements which are adapted into the approach constantly.
    - **'Lessons learned'** gathered and consolidated after each deployment. This more structured feedback is presented back to the programme as shared intelligence to ensure wherever possible improvements can be made.
    - **Survey** – Surveys are routinely conducted of users after they have been through the process of onboarding to MoJ Official. These surveys ask about all aspects of the experience from the technology through to the process of onboarding. This feedback is consolidated with our own direct experiences to continually feed into

iterative programme improvements.

i.e.

User Satisfaction KPI	Target
Good	99% or better (or zero complaints)
Approaching Target	98.9% to 95% (or minor complaints)
Inadequate	Below 95%* (or significant complaints reported)
Mitigations and actions related to critical feedback should be remedied and reported as soon as is practical *	

- **Training KPI**: The Supplier will deliver familiarisation and adoption training to a minimum percentage of staff at each site, on the understanding that the Buyer will make available users for training and encourage active participation. Where users will retain legacy devices temporarily, these users will be encouraged to undergo training in the first pass of each Site to maximise efficiency and minimise costs. .

i.e.

Training KPI	Target
Good	85% of users trained (or better) completed to timeframe at a functional level
Approaching Target	Expectation of 75%-85% of users trained during engagement
Inadequate	Below 75% at completion of Site engagement *

Social Value KP (Carbon Offset): Delivery of the contract is expected to generate total CO2 emissions of 2,705,400 grams. To offset the emissions the supplier will plant 125 saplings scaled across the life of the contract. The number of saplings planted will be reported on a quarterly basis as a standing item of the management review. Reduction of the forecast emission volume by logistical efficiencies identified and implemented during delivery may also be factored in on presentation of evidence or appropriate reduction calculations.

- i.e.

SV KPI	Target
Good	-1% or more over 12 months Baseline is forecast CO2 production at start of contracted delivery
Approaching Target	-0.9% or smaller*
Inadequate	0% change or recorded increase*
Cumulative total change or specific Carbon neutral / negative actions taken in the Service Delivery may be offered as mitigations for retrospective shortfalls.	

*KPIs at these levels will require remedial plans to be made and agreed and remedial actions implemented and reported.

Weekly KPIs should be collated and reported on a Monthly basis to both to the appropriate single point of contact for Supplier dependencies and reporting and the appropriate Contract Manager for both the Buyer and Supplier. Remedial plans will be agreed through the same route with both sides acting reasonably and aiming to resolve the issues in a manner that is expedient and causes minimal further disruption.

Remedial Approach & Method to Bring Plans Back on Track

Where:

- The project is forecasting a deviation to its tolerances or
- the Buyer Governance raises a concern that any of the projects may exceed tolerance (e.g., their KPIs, quality criteria or acceptance criteria are not being met) then
- this will be notified to the Buyer Service Delivery Representative or raised as an exception to the Supplier project manager as soon as reasonably possible.

At this point the SUPPLIER project manager will assess the exception and create a remedial (exception) plan, this exception plan will then be passed to the project board and executive sponsorship for review and authorisation.

The Buyer Service Delivery representative will hold the position of Senior User in the Supplier project board for immediate communication of Supplier actions and outputs and to feed in necessary information that may impact the exception plan.

If the exception plan is approved, it will replace the stage plan with the aim to bring the prison/project back into line with the agreed tolerances.
The Supplier project manager will produce daily exception reports for Buyer for as long as the prison/project is deemed to be in exception.
The Supplier will define the service levels that the project must adhere too during the exception process with the standard SLA in place for an escalation 24 hours from the point the exception is raised to an exception plan being agreed.

It is expected that if at any point any of the Supplier's project resources fails in his or her duties that the Buyer Service Delivery representative will escalate this in writing to the project board with any available evidence for investigation. On agreement the resource will be replaced with a contingency resource and an emergency transition plan enacted.

Escalations

During project initiation, the Buyer and Supplier will agree the project structure, including the steering group committee, which will be represented by principal stakeholders including an adequate level of senior Supplier sponsorship.

For issues that cannot be rectified by the immediate project team or where the impact analysis of a critical issue forecasts a project delay outside of tolerances, the issue can be escalated to higher layers of project leadership or management. The process for this escalation is detailed in the communications plan within the project initiation document.

In this scenario, the SUPPLIER and/or Buyer project manager can raise an issue via the escalation plan to the steering group for advice and resolution. Should the issue require action from SUPPLIER, the steering group member (SUPPLIER head of project management) will agree an action plan with the board and ensure that the issue has the appropriate level of senior management support within its business to provide resolution.

Equally, should action be required within Buyer's organisation, an appropriate BUYER project sponsor can ensure this action is authorised and prioritised.

Once an action plan is agreed by the board, the escalation plan is updated with actions and owners and these are fed into the action log for tracking.

The SUPPLIER project manager will track the issue on the escalation plan and issue log, track the implementation of actions to mitigate any further delays to the project and provide reporting back to the steering group committee based on the agreed reporting methods.

Baseline Operational Methodology

Supplier engineering proposal is priced per site anticipating a full 3 weeks (15 working days) deployment time being required: Actual cost will only for resource utilised.
e.g. if a site finishes in 10 days, only 10 days resource will be billed against that site.

Expectations are that there will be in the range of 95 secure sites, subject to consolidation of or separating out satellite operational sites linked to a larger location.

A number of non-secure sites such as Satellite offices, and secure sites such as Private Prisons remain within scope, with Deployment activities for these to be agreed within the Deployment plan and through a Change Control process should these activities merit a material change to the contract.

The Buyer expectation is that the non-secure sites will require less resources and overhead to deliver than any of the Secure sites.

Engineer contingency pricing of an additional 5 days of 1 engineer per site has also been provided in the event of site rollover beyond the anticipated 15 working days required and only be billed against for the actual resource utilised.

Sites in each region are to be closely scheduled to allow for continuity and retention of engineering teams to deliver at scale and pace. The Buyer acknowledges the advantage of this approach and will work towards this outcome wherever possible during planning, operational deployment and consideration of any potential change to the deployment order.

Where scheduled project activity is delayed or cancelled at short notice, the Supplier will endeavour to redeploy the resource(s) elsewhere. If this is not possible, the Supplier may charge for the delayed/cancelled engineering and training costs of the first anticipated deployment week based on the notice days given below:

- 1 – 5 Working days' notice – 100% of daily rate for the first full week anticipated deployment

- 6 – 10 Working days' notice – 50% of daily rate for the first full week anticipated deployment.

The Buyer undertakes to confirm Change to Deployment order, removal or addition of sites as soon as these are agreed through the Buyer's internal process, on the understanding that for notice of change provided less than 10 working days before the original deployment point, these scaleable irrecoverable costs will be incurred by the Supplier and charged to the Buyer.

Communications Plan

To facilitate the smooth onboarding and delivery of the programme, The Supplier's project manager will agree a communications strategy with Buyer at the outset of the project. This will allow the Supplier and Buyer to share schedule, contingency and risk information quickly and easily across project stakeholders.

The plan will include the frequency and method for the following:

- Project meetings. An agenda will be circulated before all meetings, which can take place either face to face or by telephone. Minutes will follow the meeting with owners and deadlines for actions.

- Project reporting. Highlight reports will be issued to the required frequency summarising the status of the project, changes, risks and issues and financial reporting.

- Project control. A project RAID log will be maintained by the project manager and made available to Buyer stakeholders as needed. Change control will also be communicated as adjustments to the project scope are required.

- Project documentation. The project plan (Gantt format), PID and other documents within SUPPLIER's standard set will be provided to Buyer stakeholders and updated as needed.

- Stakeholder/RACI matrix. Defining key personnel who will review and signoff project documentation along with who will need to be consulted or informed during the project lifecycle.

- Escalation plan. Where necessary the project manager will create an escalation plan which will set out the process for escalations and name relevant personnel who will be engaged in an escalation to allow its resolution.

Contingency Planning

- The Supplier's project and resource managers will co-ordinate with Buyer and other service stakeholders to ensure that sufficient contingency plans are in place to reflect the risk tolerance of the PTTP. Foreseeable risks that can be managed and mitigated relate to several areas including:

- the impact of COVID-19,
- managing resource demands,
- the unique constraints of working in highly secure environments.

Contingency plans for these areas are addressed in detail in the attached Supplier Proposal.

Resourcing & Vetting

Vetting standards will provide the baseline security control for all personnel involved in the delivery of this project.

The Supplier will ensure that all engineers, trainers and project governance teams involved in the on site delivery of the project will be the Security Level appropriate for on-site work or access to any particular prison or site, given that different category prisons would have different access levels and vetting processes.

The Supplier project and resource management teams will be responsible for co-ordinating with each Buyer site to ensure that all documentation and evidence to support clearance activities is supplied ahead of time with the understanding that it may take between 2-4 weeks for approval to be given by each site.

The Supplier undertakes to submit records for more resources than are needed for each site to provide a pool of pre-cleared contingency resource that can be called upon at short notice.

The Supplier will make all practical use of the pool of existing SC vetted engineers that can be used to begin delivering the project immediately, recognising that:

- The Supplier would not be held accountable for delays due to Prison Sites mandating scaleable security checks dependent on Category, in addition to the Supplier's provided clearance evidence;
- During the ramp up period all trainers and engineers will be going through the MOJ Prisons vetting process;

Site Procedures

Every Supplier engineering and training team will need to be escorted at all times by Buyer personnel, and that access to/from sites is restricted to specific times throughout the day.

To maximise both the quality and speed of delivery under these conditions, SUPPLIER deployment engineers and trainers will proceed wherever possible through sites in groups. This will allow device swap outs and user training to be carried out at the same time, whilst minimising the number of escorts required to ensure the security of the service.

Agreed success factors and key performance indicators that are critical to the overall quality of outcomes to be delivered, such as:

- Completing deployment at each site within the agreed window

- Delivering familiarisation and adoption training to a minimum percentage of staff at each site (currently assumed to be between 75-80% of users)
- Providing the Buyer project team with timely and accurate asset register updates
- Maintaining compliance with each site's security and access procedures

The Supplier will promote a consistent approach through:

- Relationships: maintaining current working relationships and the understanding of how key roles and responsibilities work together to achieve the common goals
- A repeatable approach: a deployment methodology, designed and delivered around how prisons operate
- Flexibility of approach: Understanding the changing and dynamic nature of prisons, allowing for flexibility within the deployment window
- Experienced personnel: the continuation of an experienced team who have knowledge of:
    - The deployment plan and approach
    - Security clearance challenges
    - Key / radio training
    - Prison regimes and how the programme works with prison life
    - Understanding of the deliverables in terms of technology and adoption thereof
    - Data and Management Reporting: the tracking and progress to ensure delivery against aggressive timescales, providing management with a clear picture of progression against pre-agreed timescales
    - Onboarding process: an approach practised within this programme that enables the onboarding of new team members to be shadowed and supported by experienced personnel.
    - Management structure: utilising the prison deployment experienced personnel to progress into supplier management positions, supporting the regional deployment strategy. This enables guidance and an escalation point to personnel who understand the programme and the challenges of deploying Buyer Official to prisons

Quality Control and Governance Process

The Supplier will:

- use International Best Practices to assure Quality & Performance including ISO9001 and PRINCE2 Project Management methodologies.

- Assign a PRINCE2 certified senior project manager responsible for leading the project planning and for the management and delivery of the Supplier's scope of work, the quality of service and outcomes / outputs directed to the Buyer will implement a quality management and governance structure to monitor and report against the Supplier Performance.

Governance activities led by the Supplier Project Manager will include at a minimum:

- *Project definition workshop to clarify scope, constraints, resource requirement, roles and responsibilities, dependencies, assumptions, objectives, deliverables, risks and escalation paths.
- Physical output / Deliverables for sign off will include:
- *Project Initiation Document

- Project Plan
- *Initial register containing identified planning assumptions and project risks
- Weekly tracked project plan containing all resource requirements, dependencies and quality gates
- Weekly updated action register containing current actions requiring attention.
- Weekly updated assumption, risk and issue register detailing mitigating actions, levels of risk and owners
- Periodically updated change requests identifying items impacting time, cost or quality that are deemed to be outside the project scope but need to be addressed
- Weekly highlight reporting detailing the status of the project, planned work, key issues and risks and a weekly burn rate of resources against the plan (time and materials only)
- Closure reporting incorporating any lessons learned.

(* Or acceptance / continuance of the scope etc definitions arrived at during Phase I & II Deployment)

Deployment Planning and Standardised Approach

- Objectives - Key objectives upon which the deployment plan is created and executed
- Key Requirements - The key requirements which enable a repeatable and successful deployment strategy
- Deployment Plan - A working deployment methodology
- Daily Activities - The daily activities that drive the successful implementation of the deployment plan
- Training Plan – A training strategy and plan, taking into consideration the varying roles/responsibilities and how the technology will be utilised

Objectives

SUPPLIER has 3 key objectives, upon which all deployment strategy and implementations are centred:

- Delivering at scale through a repeatable model
- Minimising end user disruption to the prison regime during the change in technology
- Empower users to get the best from the new technology, enabling improved working practices

Key Requirements

The following provides the key requirements essential to build out the deployment strategy and successfully implement Buyer Official:

- Utilise the practised and repeatable methodology to minimise disruption
- Swap out all Quantum devices with Buyer Official
- Track and collect all Quantum devices ready for decommissioning
- Onboarding a target of 75-80% of users, per prison
- Create a cost-effective mechanism to support the remaining 25% of users to onboard without direct trainer interaction

- Create a sustainable footprint of digital capability / enablement
- Supporting data collection and management information requirements
- Ensure flexibility of approach, in terms of the dynamic environment in which we are deploying but also the wider plan and if required, change our approach based on COVID or wider macro factors
- Ensure consistency of experience within the deployment team to ensure efficiency, particularly among Lead Engineers and Lead Trainers to support the Deployment Manager
- Supporting users in the context of their role, helping users to get up and running with what they need as quickly as possible, creating and delivering training relevant to how they will interact with the technology

Users within the Prisons are split into 3 groups for the purpose of the Deployment and Training planning:

Non-Operational - These are users that use the technology daily as a key part of their role and are not working solely in the operational areas. This will include uniformed staff where they are not directly detailed to operational teams.

Operational - Uniformed staff detailed to work in the operational areas of the prison (Wings, Houseblocks, Segregation, Reception) where their primary role is to manage Prisoners.

OSGs (Operational Support Grade) - Due to the nature of the roles that OSGs perform on a day-to-day basis including their use of the technology and the challenge this provides in planning their onboarding, they are identified as their own cohort for planning.

Deployment Plan

The standardised approach Deployment Plan which the Supplier has and will utilise to continue to support the PTTP programme:

[REDACTED]

Daily Activities

The following describes key daily activities, along with the roles and how they interact, facilitating the successful implementation of the deployment plan.

The day before any deployment a combination of the Deployment Manager and Engineering Lead conduct a recce of the areas to be deployed to. This is carried out with a view to:

- Confirm the number of devices within the location and any anomalies e.g., unsupported screens, cables required

- Confirm with line management the personnel we are to support and any absentees
- Identify any devices that can be deployed early, providing a head start to the next day, enabling trainers and engineers start without delay in the morning

Deployment Manager and Training Lead review the data from the recce, and in line with the deployment plan identify:

- Who will be going where the next day (training and engineering)
- Which specific personnel are assigned to which tasks
- Which escorts are supporting the process

Training report back to the Deployment Manager during each day of the deployment, assigning each targeted user one of four categorisations in the data hub:

1. **Deployed** – those who have been successfully deployed to and number of devices successfully replaced on desk

2. **Bucket** – those who could not be present for onboarding, the trainer will check with the user's line manager and find out when they will next be available for onboarding, this date inputted to the data hub to enable them to be targeted at the correct time

3. **Review** – an identified issue with specific user of device to be replaced that the Deployment Manager will need to investigate

4. **Post Deployment** – the user won't be present for onboarding during the deployment lifecycle as they have left, long term sick, on secondment etc.

This consistent daily approach enables the tracking of management information to ensure the programme is progressing as required to achieve the agreed target of 75%- 80% of users onboarded during the deployment lifecycle.

Furthermore, this approach enables us to minimise disruption by identifying when users are available and specifically retargeting them at an appropriate time, rather than causing disrupting and removing them from essential duties.

[REDACTED]

Key Success Factors

1. There are several key success factors which should be called out as part of making the deployment window successful:

2. Awareness sessions for management (SMT and Band 5s) have proved to be essential in helping them understand:

    a. What is happening
    b. When it's happening
    c. What they will get from the changes
    d. Challenges they will face if not in the process
    e. How we will support them and their teams through the process

3. Approaching managers in this way enables the Deployment Team to be efficient on-site and work with them to:

    a. Clean the data i.e., who resides in their teams to be targeted
    b. Understand who is going to be present and when within their teams
    c. Make staff available for the deployment schedule

4. Tracking of progress against the Deployment Plan ensures essential organisation and fundamentally enables us to track who has and has not been onboarded. Ultimately this allows for tracking against the overall target of 75-85% of users onboarded.

5. The training team feed into the Deployment Manager, daily, where we are for each day's targeted users against 4 key categorisations:

    a. **Deployed** – those who have been successfully deployed to
    b. **Bucket** – those who could not be present for onboarding, the trainer will
        i. check with the user's line manager and find out when they will next be available for onboarding and this date is inputted to the data hub to enable them to be targeted at the correct time
    c. **Review** – an identified issue with specific users that the Deployment Manager will need to investigate
    d. **Post Deployment** – the user won't be present for onboarding during the
        i. deployment lifecycle as the have left, long term sick, on secondment etc.

6. This methodology enables all involved to stay on top of the progress against plan and ultimately enables the attainment of 75-85% of prison personnel onboarded during the deployment window.

7. Attending Custodial Manager's daily meetings integrates the deployment leads with the running of the prison regime, ensuring any issues or challenges faced by the prison can be considered when planning the deployment. This approach is widely appreciated by the Managers we have worked with in the first 4 prisons and enables a far better response and support for the deployment.

8. Repeatability and flexibility in approach is a fundamental success factor. Creating a 'cookie cutter' approach that works with prison regimes but that can be flexible based ensures we work with prison personnel to successfully deploy and onboard their users.

9. Consistency of staff, who have worked within the deployment model and understand the prison regime ensures efficiency and effectiveness of the agreed approach during a short deployment window.

10. Utilising ‘Detail’ to reconcile who is on shift and can be targeted for deployment, enables us to ensure we are as self-sufficient as possible in targeting users for onboarding and when they are available.

11. The daily recce of the next day’s deployment area, ensures that we are organised, having identified the devices and personnel to be onboarded and wherever possible deploying devices in advance to keep the schedule moving forward positively.

12. Proactive and reactive revisits to ensure we sweep though the prison, assisting users in their moment of need, negating the need for Service tickets to be raised.

13. Qualitative user feedback on completion of onboarding is essential, making sure that each trainer leaves the user with access to all the line of business applications, data and shared files they need to carry out their respective duties. Trainers actively seek verbal sign off from each user to ensure they are in a ‘good known working state’ before moving on.

14. Working as a team, particularly among the senior deployment personnel (Deployment Manager, Lead Trainer and Lead Engineer), working to support each other and enabling cover and flexibility which underpins the progression of the deployment plan.

    a. Access your personal files and data using OneDrive
    b. Access key applications
    c. Import favourites and adding new ones
    d. Introduction to new applications e.g., Microsoft Teams
    e. Assistance with accessing Outlook and signatures

15. In a number of sites in earlier phases evening training has been a useful addendum for those semi-permanent night-shift staff that use the services.
    a. Where agreed operationally on a Site-by-Site basis this is in scope as an exceptional service option per site. Where additional non-standard costs are incurred in delivery the per-site FTE contingency may be used if available. In any event one-of non-standard training exercises will be in scope of the contract’s contingency funding on agreement with the Buyer’s operational governance.

Training Plan

The training plan has two key elements that ensure we successfully engage with users to ensure they get the best from the technology:

- **Onboarding** - Onboard users to the technology, managing the change and minimising any disruption to their working day

- **Transformation** - Ensure users get the best from the technology, developing their capabilities to underpin improved working practices

Onboarding

As depicted within the deployment plan, the onboarding of users is highly planned and agreed with the prison hierarchy. There are 6 key elements which support the onboarding process:

Training and Awareness Sessions – These sessions are designed utilising the key principles of Change Management, creating key perceptions in users. Each of us come at changes in technology with a different feeling, some will embrace however for many it will be approached with trepidation, and even avoidance.

As a result, we run planned sessions which help users understand:

- What the change is
- Why it is happening
- How they will be positively impacted
- How they will be supported through the process

This approach levels everyone's knowledge and prevents users creating their own perceptions around how intimidating, and or difficult the process may be. This mental preparation provides comfort with the process and helps users understand how they'll be supported throughout. This has proved invaluable in aiding the high attendance rates in user onboarding sessions, and therefore drives the effectiveness of the deployment strategy.

Deployment – This is the physical onboarding of users to their new devices; this can be laptops or desktop devices.

- **Laptops** – The vast experience of supporting Phase 1 and Phase 2 means we have developed a practiced methodology enabling laptop users to be onboarded either on premise or remotely. The advantage to remote onboarding is that multiple users and or prisons can be supported simultaneously by a central function empowering scale deployments from a training perspective whilst ensuring the desired outcome.

- **Desktops** – Supporting users on premise with desktop device onboarding is designed to be as efficient as possible and our experienced team tailor their approach based on the role of the individual they are working with. The trainer's goal at this stage is to help the user get up and running and ensure they have access to all the information, applications, drives and data they need

to continue working, creating a familiar and comfortable working environment for the user. This is achieved in small user groups or on a 1-2-1 basis.

The trainers support users (laptop or desktop) in their moment of need with:

- Login processes
- Access to line of business applications
- Mapping shared drives
- Accessing personal files and data
- Introduction to new operating system
- Introduction to new apps
- Printer configuration

Revisit - After the initial onboarding, users are in a good working state and left to continue with their working day. Our team proactively circle back at intermittent periods, providing a floorwalking service to support users as they get to grips with the new technology and set up.

On-demand – Users can recall a floorwalker/trainer on-demand to support them with any 'how to' related queries as they practically get to grips with using the technology during the deployment window. Supporting users in this way enables us to capture any challenges upfront in advance of future deployments, preventing the reliance on support services.

Transformational Training – In order to minimise the impact on the working regime of the prison and to enable users to develop their skills, knowledge and understanding of the new technology, we will run a series of tailored training sessions, remotely utilising the new technology (Teams).

If all the training was to be delivered all at once during the deployment lifecycle it would take staff away from important tasks and negatively impact the running of the prison. Furthermore, users attempting to digest the required training in such a short period of time would not make for effective knowledge transfer.

Training sessions will be run centrally and can serve multiple prisons at once creating a cost-effective enablement solution for the Buyer. These sessions will be run on a loop, enabling prison personnel to book themselves onto sessions around their own diaries, again minimising disruption which provides the opportunity to learn and develop their digital skills.

The image on the right provides an overview of the training that will be conducted. This training focuses on the key features and function of new apps (Teams OneDrive & SharePoint) but tailored for the varying needs of operational and non-operational staff.

Key to the delivery of this training is the contextualisation of how the varying features and

functions will be applied within operational and non-operational roles.

Providing context in this way when training enables the user to visualise immediately how the technology applies to them and how they will work. It is also proven to drive up retention, enabling the user to attach new learning to already stored information within their memories, significantly aiding recall. This contextualisation will continue to evolve as the technology is utilised and new and improved practices are developed.

Sustainable – There are 3 key factors which make it essential to provide a sustainable footprint of digital capability within each prison and a mechanism to support the ongoing development of how the technology is used:

1. It is not possible, due to the nature of the facilities, shift patterns etc to get to 100% of users during a deployment cycle and therefore supporting mechanisms needs to be in place to help these users once we are no longer onsite

2. Staff turnover in prison settings can be high and our deployment cycle is a window in time, new starters will need assistance to get to grips with the technology, fitting into newly developed working practices

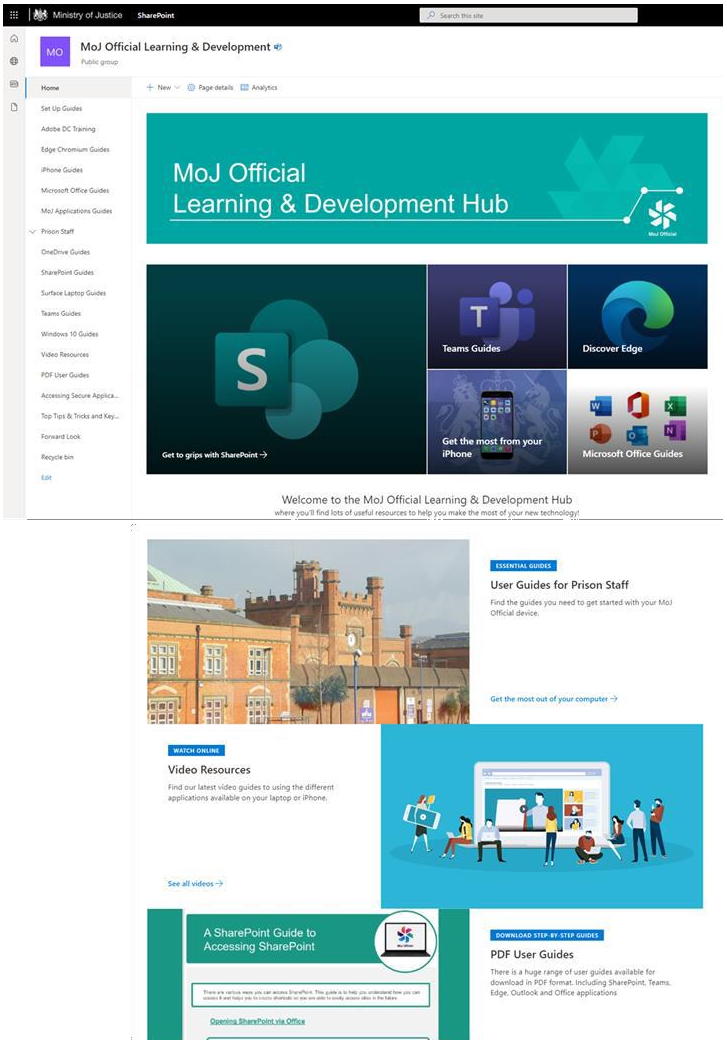
3. New applications such as the Microsoft Suite will continually evolve with new features and functions, providing further opportunities for users to get the best from the technology

As part of the deployment, we will train a network of Champions, providing a supporting central, cost-effective mechanism which empowers the programme's sustainability. This central function will support all prisons at the same time, utilising the Buyer Official technology, helping to ensure costs are kept to a minimum while providing consistently high-quality, ongoing enablement.

The diagram below describes the key functions the central Champions function will provide, keeping the network, energised, relevant and of tangible benefit to the prison service.

Knowledge Hub – The Knowledge Hub is a resource created and managed by SUPPLIER, it is a central repository for 'how to' guidance on a plethora of subjects relating directly to Buyer Official, supporting users and Champions, content includes:

- Onboarding
- Microsoft Teams
- SharePoint
- OneDrive
- Adobe DC
- Edge Chromium
- Microsoft Office Guides
- Surface Laptop guides
- Windows 10 guides
- Top tips and Tricks



The content comprises of PDF guides and videos supporting users with information on how to get the best from the new technology. The content is kept up to date by the same team who are training and enabling users so are industry experts in the technology.

This will allow device swap outs and user training to be carried out at the same time, whilst minimising the number of escorts required to ensure the security of the service.

SUPPLIER's resource and capacity plans have been developed based upon the above approach which has been refined based on our experience of delivering previous stages of this project. Our expectation is that this will provide a more accurate forecast of project costs for the Buyer team – as well as a more credible demonstration of how the project can be completed within the required timeframes.

The Supplier will ensure that a minimum of 50% of onsite resources have previously delivered PTTP activities ensuring seamless knowledge transfer and consistent delivery throughout Phase 3.

Milestone Plan & Dependencies on PTTP Project Team

This section is the *de facto* initial SOW. The table below details the steps SUPPLIER will take to commence work within 8 weeks of project award. These steps consider our experience delivering Phase 2 of PTTP. Where possible, we have identified any dependencies we have on Buyer for information or resources that will allow us to meet the stated timescales.

[REDACTED]

Service Options (Regulation 72 Pre-Defined Changes)

Dual Mode PC Option: The Supplier acknowledges that the option to utilise Dual Mode PC to accelerate device deployment is feasible (with Adoption following on behind in slightly longer time.) However it is recognised that Supplier engineers have a dependency on guidance of the Lead Trainer and Deployment Manager and that the redirection of the Deployment Manager would create disruption for the prison operationally. Under these circumstances the Site would require 2 deployment lifecycles to be run rather than one.

SharePoint Online Training Option: This will remain in scope of the contract although at the point of Contract signature this is not being actioned. Should this option be required this option must be to be activated through an Agreed Change Control in the process appropriate to this contract.

Training Hub Transition to BAU Support Option:
Should the Buyer have an ongoing requirement to provide end user training through the Deployment Training Hub model as part of BAU activities, the Supplier will on request define and cost an independent training service to baseline the cost of this requirement.

Should the Buyer choose to deliver this function internally or through a 3rd party the Buyer will provide the necessary user rights, documents, collaterals and processes created in the delivery and enablement of the Buyer Programme as part of project exit, knowledge transfer and general handover activities. The agreed aim is to ensure Buyer does not incur any proprietary or technical debt, reduce the time and labour required to establish the new training function, and provide a known baseline for service quality and continuity.

Second Round Site Activities ("Washup" Activities)

There is an expectation that approximately 10% of legacy Devices ("Quantum") and their users will remain operational after the first pass of the Site engagement until a designated point in the Deployment Plan. Where feasible and made available users of these legacy devices should be encouraged to undergo training in the first pass of each Site to maximise efficiency.

On Agreement through an appropriate Change Control Process, the Supplier will undertake a secondary replacement exercise across the designated Sites and swap out those devices to the same level of effectiveness as in the first Engagement round. Buyer expectation is that the on-site duration expectations for this secondary engagement will be minimal, but may require both Engineering and training services dependant on the outcomes of the first round at each Site.

Schedule 2: Call-Off Contract charges

Summary of Indicative Charges

[REDACTED]

[REDACTED]

[REDACTED]

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

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

2. Incorporation of terms

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

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

- 8.59 to 8.60 (Data protection
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

5.1.4 have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

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

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

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

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

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

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

11.7.3 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

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

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

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

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

13.6.6 buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

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

21.6.1 the Buyer will be able to transfer the Services to a replacement Supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement Supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

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

24. Liability

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

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

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

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement

29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

29.6.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 3: Collaboration agreement

Not 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	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.

Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)

DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A Supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.

GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium

Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the Supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.

Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.

Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.
Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: o under the Bribery Act 2010 o under legislation creating offences concerning Fraud o at common Law concerning Fraud o committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.

Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.

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

Schedule 7: GDPR Information

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

Annex 1: Processing Personal Data

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

1.1 1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]
(a) Post Point 11.52, 102 Petty France, London SW1H 9AJ

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

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	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ● [**Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer**] **The Supplier is Controller and the Buyer is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data: ● [**Insert the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier**]

	The Parties are Joint Controllers The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: [**Insert the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together**] **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● 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 ● [**Insert the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer**] [Guidance where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]
Duration of the Processing	[**Clearly set out the duration of the Processing including dates**]
Nature and purposes of the Processing	[**Please be as specific as possible, but make sure that you cover all intended purposes**.

	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment Processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	[**Enter type of Personal Data.** Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[**Enter categories.** Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, Suppliers, patients, students / pupils, members of the public, users of a particular website etc]
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	[**Describe how long the data will be retained for, how it be returned or destroyed**]

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 4 of the Framework Agreement (Where one Party is Controller and the other Party is Processor) and paragraphs 17-27 of Schedule 4 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [**delete as appropriate Supplier/Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**Supplier's/Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a data subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

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

(a) report to the other Party every **[enter number]** months on:

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

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

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

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

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

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

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses

2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

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

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

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

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

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

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

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

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

(i) nature of the data to be protected;
(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

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

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.