



Crown Commercial Service

G-Cloud 12 Call-Off Contract - Service Design and Change Management Managed Service

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

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

Part A: Order Form

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

Digital Marketplace service ID number	Service design in Justice (Service ID 842766391833498) Business change management in Justice (Service ID 869481658210940)
Call-Off Contract reference	Prj_5044

Call-Off Contract title	Service Design and Change Management Managed Service
Call-Off Contract description	The provision of a Service Design and Change Management managed service to the MoJ Electronic Monitoring Programme and Pre-Sentence Report Pilot
Start date	01/04/2021
Expiry date	31/03/2022 This Contract sets the maximum duration of term only and does not make commitment on behalf of the Parties to any length of term.
Call-Off Contract value	Up to £3,558,924 (= £2,965,770 + 20% Contingency £593,154) This Contract sets the maximum value only and does not make commitment on behalf of the Parties to any minimum spend
Charging method	This is a Call-Off contract and the following charging methods will be determined through the Statement of Works (SOW). 1 Capped Time and Materials (CTM) 2 Incremental Fixed Price 3 Time and Materials (T&M) 4 % Retainer 5 Fixed Price 6 A combination of two or more of the above Charging methods]
Purchase order number	To be confirmed after contract signature

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12). Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

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

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

From the Buyer	The Secretary of State for Justice (Ministry of Justice) [REDACTED] Buyer's main address: 102 Petty France London SW1H 9AJ
To the Supplier	Clarasys Limited 020 3811 4976 Supplier's address: Hatfield House, 52-54 Stamford St, South Bank, London SE1 9LX Company number: 07311129
Together the 'Parties'	

Principal contact details

For the Buyer:

Commercial

Title: Commercial Manager

[REDACTED]

Operational

Title: Head of PMO

[REDACTED]

For the Supplier:

Title: Director

[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01/04/2021 and is valid until 31/03/2022
-------------------	---

Ending (termination)	<p>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).</p> <p>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).</p>
Extension period	<p>This Call-off Contract can be extended by the Buyer for 2 period(s) of up to 12 months each, by giving the Supplier 30 days written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p> <p>The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.</p> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p>https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</p>

Buyer contractual details

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

G-Cloud lot	<p>This Call-Off Contract is for the provision of Services under Lot 3: Cloud support</p>
--------------------	---

G-Cloud services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none"> • Service design in Justice (Service ID 842766391833498) • Business change management in Justice (Service ID 869481658210940)
Additional Services	N/A
Location	The Services will be provided from the supplier site or remote working and to support collaborating working, will be co-located at the Buyer site (Ministry of Justice, 102 Petty France, London, SW1H 9AJ)
Quality standards	The quality standards required for this Call-Off Contract are outlined within Schedule 1, the Supplier's relevant G Cloud Service Offering, and the Supplier proposal.
Technical standards:	The technical standards required for this Call-Off Contract are outlined within the requirements, the Supplier's relevant G Cloud Service Offering, and the Supplier proposal.
Service level agreement:	<p>Any relevant service levels relating to activities such as those outlined in Schedule 1 will be agreed between both parties in the individual SOWs.</p> <p>These may include the delivery of artefacts such as process maps, high level designs, change plans, change materials, stakeholder / subject guides etc.</p> <p>The quality of these will be assured by:</p> <ul style="list-style-type: none"> • Internal QA: Workstream leads will meet a minimum of once a month to discuss their specific projects to align to their approaches, share knowledge and discuss ways of working. • External SME QA: Our workstream leads will validate project approaches with you supported by other product SMEs across Clarasys. They will go through project approaches on a monthly basis to make sure we are aligning with you. <p>Each SOW will include clear SLAs and/or KPIs for this service.</p>

Onboarding	<ul style="list-style-type: none"> • As the existing supplier there are no additional onboarding activities. • All Supplier Staff deployed to this Project shall possess the appropriate required Security Clearance, prior to the commencement of any work. • The Supplier shall, throughout the life of this Contract, be responsible for undertaking appropriate internal mobilisation to ensure consistent and streamlined supplier staff deployment.
Offboarding	<p>The offboarding plan for this Call-Off Contract is to be defined and agreed within a Statement of Work (SOW) issued within the life of this Contract, as and when required. 6 months prior to the expiry of this contract (March 2022) or when required by the Buyer, the Supplier must provide the Buyer with an exit plan for approval by the Buyer.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Any exit activities will be agreed via the SOW.</p>
Collaboration agreement	<p>Within the life of this Contract, a collaboration agreement may be implemented if and when required, subject to agreement between the Parties, and shall be executed via a Contract Change Notice (CCN).</p>

Limit on Parties' liability	<p>The annual total liability of either Party for all Property defaults will not exceed 125% of the total Charges paid by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability for Buyer Data defaults will not exceed 125% of the Charges paid by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability for all other defaults will not exceed 125% of the Charges paid by the Buyer to the Supplier during the Call-Off Contract Term.</p>
Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> • A minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract • Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • Employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 28 consecutive days.</p>
Audit	<p>No additional over and above those provisions set out in G-Cloud 12 Framework Agreement clauses 7.4 to 7.13</p>
Buyer's responsibilities	<p>The Buyer is responsible for the provision, setup and onboarding of required IT equipment and system access for all relevant Supplier Key Staff.</p> <p>Buyer Policy Note - Buyer policy is to restrict external systems access to shared files relating to the programme, and the transfer of certain files between personnel supporting the programme can only involve email if the email accounts are within the Buyer's own domain. Therefore, the services cannot be provided solely on the Supplier's equipment. Buyer equipment will be returned to the Buyer at the end of the period within which the Supplier's service are provided. If the</p>

	buyer does not provide any laptops the supplier may use their IT and email via CJSM secure email to mitigate the risk.
Buyer's equipment	The Buyer will provide laptops for the sole purpose of Supplier Staff to operate within the Buyer Policy Note (above)

Supplier's information

Subcontractors or partners	<p>The following subcontractor will be used to deliver the service.</p> <p>[REDACTED]</p> <p>Within the life of this Contract, other Supplier subcontractors or partners may be identified if and when required, subject to agreement between the Parties, and shall be executed via a Contract Change Notice (CCN).</p>
-----------------------------------	---

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS.
-----------------------	--

Payment profile	<p>The payment profile for this Call-Off Contract is monthly in arrears, based on actual usage.</p> <p>The SOW will call out the payment profile for that piece of work, which may include but not limited to Capped Time and Materials (CTM), Incremental Fixed Price, Time and Materials (T&M), % Retainer, Fixed Price, A combination of two or more of the above Charging methods etc</p>
Invoice details	<p>The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.</p>
Who and where to send invoices to	<p>Invoices will be sent to [REDACTED]</p>
Invoice information required	<p>All invoices must include</p> <ul style="list-style-type: none"> • Timesheets • SOW reference • PO number • Acceptance Certificate where stated in the SOW
Invoice frequency	<p>Invoice will be sent to the Buyer monthly.</p>
Call-Off Contract value	<p>The total value of this Call-Off Contract is £3,558,924</p> <p>This was calculated by the total value of the estimated resource outlined in schedule 1 (£2,965,770) plus a 20% contingency.</p>
Call-Off Contract charges	<p>The full breakdown of the Charges is provided in Schedule 2 of this Contract. A summary of the charges is listed below:</p> <p>[REDACTED]</p>

Additional Buyer terms

Performance of the Service and Deliverables	<p>An implementation plan, exit and offboarding plans and milestones may be implemented as and when required within the life of this Contract, defined and agreed within an SOW. Clarasys will ensure this service is provided to the highest standard to the buyer by:</p>
--	---

- Hosting monthly meetings with nominated senior business representatives and our account leads to proactively look at upcoming demand and ensuring the appropriate supplier staff are available.
- Running monthly planning exercises with workstream leads to ensure that we are always aligned with the buyers' priorities.
- Reviewing previous month's plans with workstream leads to ensure all outcomes were delivered to a satisfactory standard.
- Providing weekly workstream reports to workstream leads outlining key activities completed, plans for the following week, risk and issues and any upcoming resource annual leave.
- Hosting internal quality review sessions with Clarasys design and change SMEs to de-risk delivery and bring innovation and best practise to the way we work.
- Providing monthly updates against the additional value for money proposal.

The Key Performance Indicators for this contract are as follows:

KPI 1 – Performance to Pay

In accordance with the agreed performance to pay process, the supplier to submit the following 'inputs':

- Accurate and complete invoicing and invoice back up information (including where necessary timesheets) in a timely manner
- Accurate and complete Acceptance Certificates in a timely manner
- Accurate and complete Supplier Reports in a timely manner
- Accurate and complete invoices in a timely manner

Measurement:

Green – All of the inputs are submitted in accordance with the performance to pay process timescales and contain accurate and complete information

Amber – Inputs are later than prescribed in the performance to pay process but within 5 working days of the prescribed dates and/or inputs are incomplete and inaccurate.

Red – Inputs are later than 5 working days in the prescribed performance to pay process and/or input contains significant errors.

	<p>Source: Supplier reports/invoices Owner: TBA</p> <p><u>KPI 2 – Partnering Behaviours and Added Value</u></p> <p>The Supplier will promote positive collaborative working relationships within and across team by acting in a transparent manner. Supplier shows commitment to Buyer goals through adding value over and above the provision of compensated skilled personnel/facilitates.</p> <p>Measurement:</p> <p>Green</p> <ol style="list-style-type: none"> 1. No behavioural problems identified 2. Buyer workshops attended and positive contributions made 3. Added value recognised by the programme above provision of compensated skilled resources/facilities above compensated skilled resources/facilities. <p>Amber</p> <ol style="list-style-type: none"> 1. Some minor behavioural problems 2. Supplier only attends some workshops or provides minor contributions 3. Supplier adds some value above provision of compensated skilled resources/facilities above compensated skilled resources/facilities, but this is not regarded as significant. <p>Red</p> <ol style="list-style-type: none"> 1. Significant behavioural problems 2. Supplier contributions are rare or insignificant and shows little interest in working with other suppliers 3. No added value contributions recognised by Programme <p>Source: Monthly report and collective feedback on suppliers from both the Buyer and other Supplier staff Owner: TBA</p> <p><u>KPI 3 – Supplier Staff</u></p> <p>Successful recruitment and placement of key roles to meet the planned deliverables and contractual obligations, the supplier proactively manages their supplier staff/resource skill set and facilities by identifying issues early and in a timely fashion addressing to ensure the smooth delivery of the service.</p>
--	--

	<p>Measure:</p> <p>Green - targets meant for all supplier staff and bringing on any new supplier staff with a maximum of 14 days notice.</p> <p>Amber - target met for most 50% plus resources/ facilities through no fault of the buyer</p> <p>Red - target missed for most resources' facilities requested through no fault of the buyer</p> <p>Source: Monthly reporting and other Supplier staff feedback Owner: TBA</p> <p><u>KPI 4 – People in place (Delivery)</u> All supplier staff delivering service for the contract are performing to the expected standard for the skill set supplied are to the expected standard</p> <p>Measurement:</p> <p>Green</p> <ol style="list-style-type: none"> 1. No resources are swapped out due to deficiency in skillset 2. No problems identified with the quality of the work 3. Supplier is making positive team contributions 4. Supplier skills meet the standards expected. <p>Amber</p> <ol style="list-style-type: none"> 1. Minor issues noted with quality of work 2. Few contributions made within the team. <p>Red</p> <ol style="list-style-type: none"> 1. Resource is swapped out from project due to deficiency in skill set 2. Persistent issues with quality of work (may be minor issues that have persisted from one month to another) 3. Significant issues with Quality of work. <p>Source: Monthly reporting</p> <p>Owner: TBA</p> <p>The Supplier will provide a monthly report against these KPIs.</p> <p>The monthly meeting will report any problems with the delivery of the services and any issues reported via the SOWs The Supplier will address any Supplier issues in a timely manner and at its own cost, where the issue is deemed to be sole control of Clarasys.</p>
--	---

Guarantee	N/A
Warranties, representations	No additional warranties required
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	Insurance Clause 9.3 has been amended and agreed between Parties. Buyer non-payment clause 18.6 added in supplier rights to suspend services
Public Services Network (PSN)	N/A
Personal Data and Data Subjects	N/A

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

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

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

Schedule 1: Services

This contract relates to the provision of a Service Design and Change Management managed service provided by Clarsys to the Ministry of Justice for the Electronic Monitoring Programme and NPS PSR Pilot.

Clarsys will ensure this service is provided to the highest standard to the buyer by:

- Hosting monthly meetings with nominated senior business representatives and our account leads to proactively look at upcoming demand.
- Running monthly planning exercises with workstream leads to ensure that we are always aligned with the buyers' priorities.
- Reviewing previous month's plans with workstream leads to ensure all outcomes were delivered to a satisfactory standard.
- Providing weekly workstream reports to workstream leads outlining key activities completed, plans for the following week and risk and issues.
- Hosting internal quality review sessions with Clarasys design and change SMEs to de-risk delivery and bring innovation and best practise to the way we work.

Clarasys will ensure the Service Design and Change Management service will meet the needs of the programme through its onboarding of supplier staff by:

- Committing to always being able to bring on new resources with a maximum of 14 days notice
- Providing all new resources an extensive onboarding that will cover:
 - The history of the project they are joining and how this fits into the wider criminal justice system
 - The various programme workstreams and the work Clarasys have been doing
 - Any project team documentation which is not confidential (e.g. organisational structure, team project plans)
 - Walk-throughs with existing team members on relevant subject areas
 - Relevant Ministry of Justice governance and technical processes that will be required in the role
 - Collaborative ways of working between us, the Ministry of Justice and other suppliers

- Providing ongoing coaching for one month when an internal member of staff takes on one of our roles

Clarasys will ensure collaboration with the Ministry of Justice and their suppliers with the EM Programme by:

- Hosting monthly meetings with nominated senior business representatives and Clarasys account leads to establish and monitor collaborative ways of working.
- Running monthly planning exercises with workstream leads to ensure that we are collaboratively agreeing on upcoming priorities
- Fully brief all new Authority resources on relevant collaborative ways of working within their workstream area

Due to the nature of the service and dependency to work in an agile and collaborative partnership with the EM programme, the exact outcomes and activities within the above framework / governance structure will be defined in Statements of work (SOW) agreed with the EM programme over the duration of the contract, but may include:

1. Electronic Monitoring - Legacy Programme

The future of the Legacy programme is currently uncertain. Alongside the activities listed below both the Clarasys design and business change team currently on the project will be required to support the decision with whether or not to proceed with the Legacy programme.

1.1 Key activities if Legacy programme is progressed

Design

- **SME of design**
 - Clarasys will continue to provide expertise relating to the service design.
 - Support the testing workstream (in their management of defects and definition of testing scenarios).
 - Clarify details of the service for the change team (to ensure their comms for stakeholders are accurate).
 - Work with Authority suppliers to support their development work as required.
- **Further design work** - Potential sources of this include:
 - **Test workstream**
 - Provide further design work where necessary to facilitate the resolution of defects
 - Support with further design work, pending stakeholder feedback from the portal and iframe UAT.
 - Lead on building, clarifying and resolving misinterpretations in supplier implementation.
 - **Policy changes**
 - Respond to any policy changes that impact the programme by carrying out the necessary design work, to ensure that the service supports all required order types and legislation.
 - Draft, submit and manage change requests and subsequent impact assessments.
 - **Contract management reporting**
 - Define reports and processes with the necessary MoJ team and suppliers to outline how service level agreements and Contracted Deliverable Indicators (CDIs) will be tracked and managed in the new world service.
 - Develop supporting materials and communications to facilitate an agreement between colleagues in service management, the ICF and the contract management team.
 - **Transition support**

- Support in defining the operational processes that may differ during dual running phases of transition.
 - Provide all necessary design activity to the transition workstream.
- **Maintenance of design documentation**
 - Supply updated baselines of key design documentation that is owned by the MoJ (e.g. business processes, integrated high-level design, disaster recovery processes).
 - Update relevant MoJ design documentation following stakeholder feedback or policy changes (e.g. business processes and the integrated high-level design).
 - Quality assurance provided to revised documentation supplied by the Lots.

Business change

- **Input into the New Service design (new service and portal)**
 - Work alongside the design and UAT team to provide a Business change and business impact view on all raised defects, to ensure the new service (and portal) is fit for purpose for our stakeholders.
 - Review and revise the Change Impact Assessment on both the new service and portal to effectively shape training and comms for various stakeholder groups.
 - Conduct a benefits analysis of the portal/ new service to ensure effective positioning and buy-in with various stakeholder groups.
- **UAT Cycle 3 (new service and portal)**
 - Work alongside the UAT team to plan the UAT approach and ensure that the external UAT stakeholders are appropriately selected, engaged with and onboarded, to ensure a successful UAT cycle.
 - Design a specific UAT comms plan (for new service and portal) and produce supporting materials to create a positive UAT experience for all stakeholders.
 - Work closely with Lot 1 to create a User/ Admin Guide to support the UAT process for stakeholders.
 - Design and deliver expert UAT support.
- **Training and collateral**
 - Conduct a training needs analysis for “committed” stakeholders in order to ensure that training and resources are tailored to their individual needs and interests.
 - Work with Lot 1 to ensure feedback for External UAT is reflected in the User/ Admin Guide.
 - Create training collateral for stakeholders e.g. role-specific guides, FAQ document and scenario-based online training videos.
 - Create engaging training materials (e.g. interactive guide), to support with train-the-trainer sessions provided by Lot 1, across stakeholder groups.
 - Support Lot 1 in coordinating and running five portal train-the trainer sessions with stakeholder SMEs.
- **Communications and engagement (new service and portal)**
 - Create a new service/ portal awareness comms approach that will target all impacted stakeholders and raise the profile of the portal launch.
 - Create and deploy all comms collateral, using a variety of platforms.
- **Go-live and readiness activities**
 - Conduct a new service readiness assessment to ensure that the Authority and impacted stakeholders are ready for the new service go-live.
 - Update relevant stakeholder documentation/ resources to reflect changes as part of the portal.
 - Collate and share a list of portal user information, to ensure a smooth day one transition.
 - Collate and share all resources/ documentation to be uploaded to the portal prior to go-live, to ensure a smooth day one transition.
- **Soft launch deployment**
 - Deliver hypercare service to readily respond to questions/ issues from end-users. This will allow us to quickly identify required changes/ questions whilst still testing the new service and processes.

- Collect objective/ subjective feedback on the new process to identify any urgent changes needed before national launch. This includes:
 - Collecting end-user feedback through our Business change Leads and surveys/ focus groups on satisfaction with the process, portal and new service benefits.
 - Measuring quantitative metrics including portal uptake, order accuracy and other agreed KPIs.
- **National launch deployment**
 - Amend the portal/ new service go-live comms approach based on feedback from soft launch.
 - We will continue to collect objective/ subjective feedback and data to identify improvements, drive uptake and create EM case studies. This includes:
 - Collecting end-user feedback through our Business change leads as well as surveys and focus groups on satisfaction with the process, portal and new service benefits.
 - Measuring quantitative metrics including portal uptake, order accuracy and other agreed KPIs.
- **Transition support**
 - Ensure all internal documentation and processes are updated to reflect the new EM service/ portal.
 - Ensure internal SMEs are established and communicated across the business.
 - Ensure “project-based” processes and forums are effectively handed over and/ or closed down, to avoid confusion or inefficiencies.
 - Ensure that open items are handed over with a clear action plan (i.e approach to stakeholder groups who may wish to use the portal in the future).

1.2 Key activities if Legacy programme is stood down

In the event of the legacy programme being stood down there are a number of design and change activities that will have to be carried out. These will be scoped out in more detail as the strategic direction of the programme is determined in the coming months, however, below is a high level summary of these activities.

Design - Clarasys estimate work will be required on the following activities in the instance that the legacy programme is stood down:

- Contribute to ongoing design decisions around the EM expansion case management system in the absence of Gemini.
- Potential requirement to run an as-is process mapping exercise to get a better understanding of bridge service to scope out potential improvements.
- Support requirement gathering for any new procurement exercises required as a result of standing down current new world suppliers.

Business change - Given the ongoing open questions regarding what will replace the portal if the Legacy programme is stood down, Clarasys are proposing Change Management services will be required to support in the closure of the Legacy programme and to feed into future discussions and development of its replacement (e.g. a new “portal”), as well as inputting into other improvements to the service. Specific activities would be confirmed as clarity on the future direction after Legacy is provided but include:

- Document and share learnings and insight from the Legacy programme.
- Draft and distribute stakeholder facing comms to key EM stakeholders regarding the closure of the Legacy programme and what this means for them and the EM service.
- Support all programme close down activities.
- Identification of key improvements that should be pursued in the absence of the new service, based on insights from Legacy.
- Support in the scoping, ratifying and design of a future EM stakeholder-facing portal, based on insights from Legacy

2 Electronic Monitoring - Alcohol Monitoring

2.1 Design milestones and activities

AAMR:

- **Embed AAMR across England**
 - Management and handling of design queries and support post roll-out.
 - Provide quality assurance of EMS service uplift work to ensure it meets MoJ standards.
 - Handover and upskill CMT, Service Management and ICF for Acceptance into Service
 - Facilitate the transition in the AM service (SCRAMnet) for the Probation Reform Programme.
 - Support the Policy Evaluation work to understand the long term impact of AAMR on service users.
 - Review additional requirements to increase the EMS CMS capacity ahead of development and set up a process for improvements for the AM service to be identified, prioritised and agreed/rejected based on benefit.
- **Market engagement and strategic procurement**
 - Availability of design SME knowledge for Procurement's market engagement strategy, to assist in deciding on the preferred long term supplier of both field services and monitoring services.
 - Allocate design input for strategic procurement activities.

AML:

- **Preparation for Wales go-live**
 - Define, document and agree AML processes.
Agree and document additional requirements for AMS and EMS.
 - Design AML Target Operating Model and High Level Design as well as changes to other design documents (e.g. business rules) as required.
 - Define external systems updates required for AML.
 - Facilitate commercial activities and updates to the AM commercial documents.
 - Support end-to-end UAT preparations including test script writing.
- **Preparation for England go-live**
 - Identify Design Lessons Learned from Wales go-live.
 - Update AMS and EMS requirements as required following Wales go-live.
 - Revise commercial documentation to cover AML England roll-out.
 - Support with the end-to-end UAT activities.
- **AAMR out of court disposals/expansion/migrating to strategic solution/change of tag supplier - if required**
 - Service design for Out of Court Disposals using AM design as starting point
 - Updates to design work to extend AAMR lengths
 - Updates to design for moving AM to a strategic solution
 - Updating the design for AM to account for the introduction of a new equipment supplier

2.2 Change milestones and activities

AAMR:

- **Embed AAMR across England**
 - Ensure long-term stakeholder support channels are in place.
 - Refresher training and support materials for new joiners.
 - Ensure mechanisms are set up to track, measures and respond to MI reporting.
 - Upskill and support the ICF team so they can continue with stakeholder engagement and drive continuous improvement.

AML:

- **Preparation for Wales go-live**
 - Support IOM with identification of local SPOCs to support roll-out and engagement.
 - Preparation of Wales briefing materials & guidance documentation.

- Obtain stakeholder buy-in and raise awareness amongst stakeholders.
- Carry out virtual briefings and other initiatives to engage and upskill stakeholders.
- Create training and communication materials for Wales Probation and Prison staff
- Development of E-learning module for AML.
- Work with the press office and internal comms to define and draft communications for Wales launch.
- Support design team in defining processes that involve stakeholders and identifying changes to stakeholder IT systems, so that changes are made in time for go-live.
- Help the test team with assessing that processes and systems are fit for purpose, and meet the needs of stakeholders.
- Identify management information needs prior to go-live.
- **Wales go-live & initial operation**
 - Publish tailored comms to launch AML across relevant channels.
 - Drive uptake and assess performance of the service through evaluating MI and feedback.
 - Carry out direct engagement with Probation and Prison staff as and when a potential AML condition is identified.
 - Collate and publish case studies and success stories.
 - Carry out post-implementation review of the process and training.
- **Preparation for England go-live**
 - Work with Probation to ensure timelines align with the reunification programme.
 - Support IOM with identification of local SPOCs to support roll-out engagement.
 - Update briefing, training and communication materials for England Probation and Prisons to reflect feedback from Wales go-live.
 - Carry out training and engagement sessions to all stakeholder groups impacted
 - Work with press office and internal comms to define and draft communications for launch (including Wales success stories).
- **England go-live**
 - Publish tailored comms to launch AML across relevant channels.
 - Drive uptake and assess performance of the service through evaluating MI and feedback.
 - Carry out direct engagement with Probation and Prison staff as and when a potential AML condition is identified.
 - Collate and publish case studies and success stories.
 - Carry out post-implementation review of the process and training.
- **Embed AML**
 - Ensure long-term stakeholder support channels are in place.
 - Refresher training and support materials for new joiners.
 - Ensure mechanisms are set up to track, measures and respond to MI reporting.
 - Upskill and support the ICF team so they can continue with stakeholder engagement and drive continuous improvement.
- **Explore AM for out of court disposals/extension of AAMR/change in tag supplier/strategic solution**
 - Support Policy and Home Office colleagues to explore the benefits and implications of extending eligibility of AM to out of court disposals.
 - Identify and support change efforts required if AAMR is extended beyond the current 120 day maximum requirement.
 - Own strategy and approach for change in tag supplier and work with new supplier on re-training for impacted stakeholders

3. Electronic Monitoring - Acquisitive Crime

3.1 Design milestones and activities

- **Pathfinder initial operation and embedding**
 - Provide SME QA support to the supplier if they continue to implement any spillover items for the Pathfinder go-live.
 - Act as the POC for the supplier providing EM and GPS data.

- Define potential enhancements to the crime mapping capability, self-service portal and the regular individualised summaries.
- Review and improve the Hub's processes and service offering.
- Maintain design documentation such as the high level design and business processes.
- Conduct service assurance activities alongside the contract management team.
- Continue to provide SME support to the MoJ Hub, MI team and Business change teams.
- **Preparation for second phase go-live**
 - Continue to define potential enhancements to the crime mapping capability, self-service portal and the regular individualised summaries.
 - Prioritise enhancements and create a roadmap for the second phase of go-live.
 - Identify any pain points in the business processes and translate these into requirements to be added to the second phase of go-live roadmap.
 - Assess whether the Hub should remain delivered by HMPPS or transition to EMS. If the latter, manage the smooth transition.
 - Deliver the activities on the second phase of the go-live roadmap.
 - Define and provide support on the implementation of a long term and scalable data solution for the regular individualised summaries, crime mapping service and self-service portal offerings.
 - Maintain design documentation such as the high level design and business processes.
 - Review the performance of running the Hub in-house and provide options paper with recommendations on whether responsibilities should be transferred to EMS (and when).
 - Continue to act as the POC for the supplier providing EM and GPS data.
 - Continue to provide SME QA support to the supplier on the implementation of the enhancements of the crime mapping capability and self-service portal offering.
 - Continuing to provide SME support to the MoJ Hub, MI team and BC teams.
- **Second phase go-live and initial operation**
 - As more stakeholder feedback is received, continue to define enhancements to the offerings.
 - Develop a further enhancement roadmap based on the activities listed above.
 - Identify any further pain points of the business processes (that may have arisen due to the significant increase in cohort size) and include these on the roadmap.
 - Deliver the activities on the new offering enhancement roadmap.
 - Continue to act as the POC for the supplier providing EM and GPS data.
 - Continue to provide SME QA support to the supplier on the implementation of the enhancements of the crime mapping capability and self-service portal offering.
 - Continue to provide SME support to the MoJ Hub, MI team and Business change teams.
- **Transition (If required)**
 - Define technical and business requirements to transition onto Gemini.
 - Prioritise the requirements and develop a roadmap of transition activities.
 - Execute the roadmap activities, such as supporting with the data migration and monitoring risks.
- **Embed Acquisitive Crime**
 - Ensure design documentation such as the High Level Design and business processes are up to date.
 - Provide final design support to the MoJ Hub and MoJ MI team in their BAU activities (including any handover items).
 - Ensure long-term stakeholder support channels are in place.

3.2 Change milestones and activities

- **Pathfinder initial operation and embedding**
 - Carry out regular post-implementation reviews of the processes and training.
 - Ensure long-term stakeholder support channels are in place.
 - Refresher training and support materials for new joiners.
 - Upskill and support the ICF team so they can continue with stakeholder engagement and drive continuous improvement.

- Support evaluation activities, including focus groups and interviews, and share insight with relevant stakeholders on a regular basis.
- Gather case studies and further qualitative insights to assist policy development and evaluation.
- **Preparation for second phase go-live**
 - Identify local SPOCs to support roll-out and engagement through Probation.
 - Update briefing, training and comms materials for Probation, Prisons, Police and PPCS to reflect feedback from Pathfinder go-live.
 - Obtain stakeholder buy-in and raise awareness amongst stakeholders.
 - Carry out virtual and in person briefings and other initiatives to engage and upskill stakeholders.
 - Support design team in defining processes and capabilities that involve stakeholders
 - Support design team in identifying any changes to stakeholder IT systems and ensuring changes are made in time for go-live.
 - Support test teams in testing processes and IT are fit for purpose and meet the needs of stakeholders.
 - Identify MI needs prior to go-live.
 - Work with the press office and internal comms to define and draft communications for second phase launch (including pathfinder success stories).
 - Work with Probation to ensure timelines align with the reunification program.
 - Support across probation, evaluation, policy and IOM refresh program to decide on how Acquisitive Crime will align to IOM for the second phase.
- **Second phase go-live and initial operation**
 - Publish tailored communications for Probation, Prisons, Police and PCCS; building on existing material where appropriate.
 - Drive uptake and assess performance of the service through evaluating MI and feedback.
 - Carry out direct engagement with local Probation SPOCs to ensure the acquisitive crime licence conditions are being added where required.
 - Direct engagement with Probation and Police staff on new capabilities, and utilise MI to monitor uptake.
 - Collate and publish case studies and success stories.
- **Embed Acquisitive Crime**
 - Carry out post-implementation review of the process and training.
 - Collate and publish case studies and success stories.
 - Refresher training and support materials for new joiners.
 - Upskill and support the ICF team so they can continue with stakeholder engagement and drive continuous improvement.

4. Electronic Monitoring - Expansion Programme

4.1 Expansion milestones and activities

- **Expansion programme business case**
 - Providing Service Design and Change Management managed service to support the programme business case, with a particular focus:
 - Strategic case- supporting the definition, scoping and refinement of the expansion programme. This includes supporting the assessment of the strategic fit of the expansion work, programme objectives and strategic risks, constraints and dependencies.
 - Management programme/ project roles- how the programme will deliver on the intended outcomes, including project roles, contingency planning, governance and assurance processes.
 - Benefits management- outline of how the intended programme benefits will be measured, tracked and reported on.

- Stakeholder engagement, communication and change management- this section will detail how critical stakeholders will be identified, engaged with and involved in an ongoing basis in the programme.
- Programme Business Case presented to Authority Portfolio Board for 28 May 2020, and Investco for 21 July 2020.
- **Expansion programme setup**
 - Support the development of the programme, through workshops and strategy sessions to build out the key elements of the programme to enable the PBC to be signed off by the Investment Committee in July.
 - Support the development of the documentation in support of SR21.
- **Supporting the Reprourement strategy through**
 - Consolidate lessons learned from previous re-procurement exercises from a service design and business change perspective.
 - Facilitate discussions across the programme to produce principles and strategy for the reprourement of the service.
 - Advise on alternative means of service delivery that will be foundational to the re-procurement strategy. This will include advising on target operating model design and approach to the addition of new service lines.
 - Lead an exercise to gather user requirements from stakeholder groups to inform the operating model design, the reprourement strategy, and to inform the nature and scope of future initiatives.
- **Alignment with probation operating model**
 - Take outputs from the requirements gathering exercise to ensure closer alignment with the probation operation model, and support the introduction of strategies that will enable improved alignment on an ongoing basis moving forward.
- **Investment appraisal mechanism**
 - Support the development of an appraisal mechanism to manage a pipeline of future initiatives. This will need to be evidence-based to ensure that EM is expanded to areas that have the greatest impact.
 - Work alongside programme colleagues to determine the nature and scope of this appraisal mechanism, as well as a governance approach.
- **Alignment with EM policy**
 - Confirm the strategic case for the expansion programme, including the objectives and outlined benefits.
 - Work with policy to understand their refreshed EM policy and determine how the strategic thinking around expansion can be aligned.
 - Develop required governance and management between EM policy and the expansion programme.
 - Identify means for the expansion programme to support EM policy (eg. capture of targeted feedback, measurement of particular success factors).
- **Benefits management and tracking**
 - Definition and refinement of expansion programme benefits, including alignment with Legacy benefits.
 - Establishment of means of measurement for benefits.
 - Determine governance and regularity of benefits appraisal.
- **Scoping future initiatives**
 - Support for scoping, design, setup and delivery of future initiatives, including:
 - Domestic Abuse Prevention Order
 - Home Detention Order
 - Police voluntary tagging expansion
 - Creation of internal EM Hub (within HMPPS)
 - Inclusion of additional service lines and capabilities (eg. crime mapping)
 - Introduce means of using more intelligent use of data
- **Continued Home Office Immigration Enforcement support**
 - Support HO Satellite Tracking Services (STS) programme to:
 - Determine user needs

- Finalise business requirements
- Create change plans and approaches

5. National Probation Service - Pre-Sentence Report (PSR) Pilot

5.1 Key activities before roll-out of PSR Alternative Delivery Model (ADM) is complete

- **Design documentation**
 - Gather feedback from Senior Probation Officers and their teams.
 - Update reference guides and learning and development guides following stakeholder feedback.
 - Successfully handover final copies of guides to the PSR pilot project manager.
 - Prepare insights and recommendations report with regards to the PSR ADM and handover to PSR pilot project manager.
- **Rollout of PSR ADM**
 - Continue to drive briefings with Senior Probation Officers and their teams ahead of each go-live wave.
 - Continue to drive engagement with HMCTS, the Judiciary, CPS, Defence Community and others.
 - Work closely with MoJ Policy and the Evaluation workstream to ensure they are kept informed of each wave's progress and monitor and manage any risks and issues that may arise.
- **Hypercare**
 - Provide post go-live support as and when each wave of sites adopt the model, including drop-in calls, managing a Teams' page with SPOs, sending out and managing feedback from pulse surveys and triaging questions / requests from the PSR mailbox.
- **Project admin assistant handover**
 - Design and deliver the onboarding for the full-time NPS project admin assistant who will be replacing the Clarasys admin assistant for the remainder of the pilot. This handover will provide the new assistant with the relevant knowledge and capabilities to support the remainder of the PSR ADM rollout.
- **Learning and development**
 - Continue to support the procurement of the recommended external training providers identified earlier in the PSR pilot project.
 - Coordinate the production of 4x learning and development videos for the PSR e-learning package by our video production subcontractor (SneakGlobal)
 - Finalise the design and delivery of advocacy, communications and presentation training by our training subcontractors (Pinnacle Performance) - this will result in 20 full-day workshops delivered for probation court staff across 15 Magistrate Court sites.
- **Scheduling external training**
 - Drive the scheduling plan for all external training once training providers have been confirmed with NPS procurement.
 - Continue to plan and work with Senior Probation Officers to finalise dates for their teams.
- **E-learning checkpoints**
 - Monitor the uptake of the e-learning package work with the PSR pilot project manager to capture feedback.
 - Create a backlog of additional learning needs before the team conducts the handover in June.
- **Communications and engagement**
 - Create and monitor communications and stakeholder engagement across the go-live phase.
 - Respond to ad-hoc requests for additional communications to be created and support with any additional meetings required with stakeholders across the project.
 - Create updates for the working group, the core group and internal stakeholder groups such as the Female Offender Team.

5.2 Key activities after the PSR Alternative Delivery Model has been adopted by all pilot sites

- **Design documentation**
 - Finalise the insights and recommendations report for the PSR pilot project manager.
- **Learning and development**
 - Produce a report for the PSR pilot manager which details recommendations to manage the L&D pack beyond Clarasys - including key contacts inside and outside of the NPS who can support them.
- **Communications and engagement**
 - Write up a recommended engagement plan beyond our time on the project
 - Complete a final audit on all the communications and engagement to date, to inform the final communications and engagement handover with the PSR pilot project manager.
- **Knowledge transfer**
 - Incrementally handover to the PSR pilot project manager through effective means e.g. official Knowledge Transfer session in the final week of June to ensure any questions and / or concerns are answered.

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract.

- The maximum Charge for work performed under this Contract is up to **£3,558,924**.
- This order form does not provide any commitment to spend any value under this Contract.
- Commitment for any spend value under this Contract shall be made via a Statement of Work, that has been subject and approved by the governance controls as outlined within 'Schedule 3: Controls'.
- Once agreed and in place, a Statement of Work shall only commit the Buyer to spend the value outlined in the document itself.

All work executed under this Contract and its Statement(s) of Work shall be charged in accordance with the below table, according to the most appropriate level of Role seniority, as agreed between Parties.

[REDACTED]

The total contract value of **£3,558,924** was derived from the supplier resource plan set out in their proposal which is outlined in the table at the end of this schedule. Actual resource plan may deviate from this, and will be agreed between supplier and buyer for each statement of work.

Work conducted by the named subcontractors **[REDACTED]** will be fixed price pieces of work with payments based on completion of milestones defined in the SOWs (e.g. production of videos or delivering of training courses)

Statement(s) of Work

This Contract sets the maximum duration of term only, and does not make commitment on behalf of the Parties to any length of term.

Commitment for all terms under this Contract shall be made via a Statement of Work, that has been subject to the following governance controls:

- Buyer internal governance review
- The Buyer must obtain Budget Approval on an individual basis for each Statement of Work released under this Contract. This must be in accordance with Ministry of Justice budget delegation controls.
- Acceptance and signature by the Supplier
- The Supplier must agree and sign the Statement of Work.
- Acceptance and countersignature by the Buyer
- The Buyer must countersign the Statement of Work, in line with Ministry of Justice sign-off delegation controls.

The Buyer shall confirm the continuation of work, with formal commitment only given via the subsequent release of a Statement of Work, at least 4 weeks prior to the current Statement of Work end date.

Approach to milestones

For each EM workstream package Clarasys will agree on a monthly plan with the workstream lead. 20% of any given month's fees will be deemed at risk and tied to the successful completion and acceptance (determined solely by reference to the acceptance criteria defined in the monthly plan) of the activities and key deliverables in such a plan.

If priorities change and at the buyer's direction and the Clarasys team needs to work on another area, we will re-agree with the workstream lead the priorities for the month. Should Clarasys not complete an activity or deliverable where it is in their commercially reasonable control to do so, then payment of the fees at risk portion will be delayed until it has been completed to the buyer's satisfaction (determined solely by reference to the acceptance criteria defined in the monthly plan).

The risk of 20% of the Sellers fees applies to the completion of the activities in the monthly plan per workstream that are within their control. This does not relate to performance against KPI 1, KPI 2, KPI 3 or KPI 4 which are outlined earlier in this document in the **"Performance of the Service and Deliverables"** of the **"Additional Buyer Terms"**

Additional Value Add

Clarasys will provide the following services free of charge over the course of the contract:

- One day per month of Principal level SME support for change management
- One day per month of Principal level SME support for service design
- One discovery piece of work with a minimum value of £40,000 This will be defined as the need arises with the buyer
- Two weeks of any new supplier staff whose role lasts over 3 months

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 reasonably 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. 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.

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

The Collaboration agreement is available at

<https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

Schedule 4: Alternative clauses

The Alternative clauses are available at

<https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

Schedule 5: Guarantee

The Guarantee is available at

<https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).

Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.

Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	<p>'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.</p>
Controller	<p>Takes the meaning given in the GDPR.</p>
Crown	<p>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.</p>
Data Loss Event	<p>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.</p>
Data Protection Impact Assessment (DPIA)	<p>An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.</p>
Data Protection Legislation (DPL)	<p>Data Protection Legislation means:</p> <ul style="list-style-type: none"> (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	<p>Takes the meaning given in the GDPR</p>

Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	<p>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:</p> <p>https://www.gov.uk/guidance/check-employment-status-for-tax</p>
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	<p>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).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.12 together with the Framework Schedules.</p>
Fraud	<p>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.</p>
Freedom of Information Act or FoIA	<p>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.</p>
G-Cloud Services	<p>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.</p>

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: <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium

Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.

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

Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.
Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> 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 The contact details of the Buyer's Data Protection Officer are: **[Insert Contact details]**
- 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	<p>The Buyer is Controller and the Supplier is Processor</p> <p>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:</p> <ul style="list-style-type: none">• [Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer] <p>The Supplier is Controller and the Buyer is Processor</p> <p>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:</p> <ul style="list-style-type: none">• [Insert the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier] <p>The Parties are Joint Controllers</p>

	<p>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p>[Insert the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]</p> <p>The Parties are Independent Controllers of Personal Data</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> • Business contact details of Supplier Personnel for which the Supplier is the Controller • Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller • [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] <p>[Guidance where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]</p>
Duration of the Processing	[Clearly set out the duration of the Processing including dates]
Nature and purposes of the Processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.]</p> <p>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</p>

	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.