

# G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

**G-Cloud 13 Call-Off Contract**

Part A: Order Form 2

Part B: Terms and conditions 15

Schedule 1: Services 36

Schedule 2: Call-Off Contract charges 37

Schedule 3: Collaboration agreement 38

Schedule 4: Alternative clauses 51

Schedule 5: Guarantee 56

Schedule 6: Glossary and interpretations 65

Schedule 7: UK GDPR Information 83

Annex 1: Processing Personal Data 84

Annex 2: Joint Controller Agreement 89

# 

# 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.

|  |  |
| --- | --- |
| **Platform service ID number** | 562394980681247 |
| **Call-Off Contract reference** | Con\_5138 |
| **Call-Off Contract title** | MOG Data Migration Service |
| **Call-Off Contract description** | Data Migration Service for DSIT |
| **Start date** | 20/10/2023 |
| **Expiry date** | 31/03/2025 |
| **Call-Off Contract value** | £948,130 (exc. VAT) |

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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 Services 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** | Department for Energy Security & Net Zero  1 Victoria Street  Westminster  London  SW1H 0ET |
| **To the Supplier** | Avanade UK Limited  30 Fenchurch Street  London  EC3M 3BD  England  Company number: 04042711  020 7025 1000 |
| **Together the ‘Parties’** | |

### Principal contact details

**For the Buyer:**

Title: KIM Digital Projects Lead

Name: Helen Paul

Email: helen.paul@beis.gov.uk

Phone: 07795 808732

**For the Supplier:**

Title: Business Development Manager

Name: David Thomson

Email: d.thomson@avanade.com

Phone: 020 7025 1000

### Call-Off Contract term

|  |  |
| --- | --- |
| **Start date** | This Call-Off Contract Starts on **20/10/2023** and is valid until **31/03/2025**. |
| **Ending**  **(termination)** | The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).  The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1). |
| **Extension period** | This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier one monthwritten notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.  Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.  If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:  <https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service> |

### Buyer contractual details

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

|  |  |
| --- | --- |
| **G-Cloud Lot** | This Call-Off Contract is for the provision of Services under:   * Lot 3: Cloud support |
| **G-Cloud Services required** | The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:  The scope of this activity is a migration service to manage the migration of core ‘office productivity’ data, both user scoped and shared data, from DCMS’s environment to DSIT’s. This includes, but is not limited to, emails and documents, as well as legacy departmental record archives. It involves moving data between DCMS’s Google Workspace and DSIT’s Microsoft 365 environments, as well as potentially between Microsoft 365 to Microsoft 365 environments.  The Supplier will provide the following Work Products as part of the Services to be provided:  **Google Migration to M365 Migration Design and Approach**  Google Migration Design and Approach, including:   * Migration Approach for Google Mail & Google Drives (Personal & Shared) * Migration Scope, Risks, Assumptions & Dependencies * Migration team Roles & Responsibilities * Security Consent and Account permissions * Migration Tools & Infrastructure * Roll back * Detailed Migration Design by Phases –   + Preparation & Configuration,   + Assessment   + Execution (prepare source and target environment, Migration validation and Cutover)   **Google to M365 Migration Timeline**  Document per workload detailing the Migration timelines and waves including:   * Migration scope and migration times * Testing criteria * Migration Waves plan   **Google to M365 Migration Test Strategy and Test Cases**  A test strategy and test cases used to test the end-to-end solution.   * Google Mail * Google Drives (Personal & Shared) * Google Vault   **Google to M365 Migration Closure Report**  Document detailing open issues at the end of the migration, including:   * Introduction * Migration Solution Overview * Test approach and completion results * Migration results * Open Issues at the end of the migration   Additional information on the G-Cloud Services scope of work to be delivered by the Supplier can be found in **Schedule 1 Services.** |
| **Additional Services** | The Supplier can provide additional services such as, but not restricted to, organisational change management to support the successful delivery of this project. Any additional services will be agreed by both Parties and will require a Change Request. The Supplier T&M rate card shown in Schedule 2 will be applied. |
| **Location** | The Services will be delivered remotely with onsite work agreed as required between the parties |
| **Quality Standards** | The quality standards required for this Call-Off Contract are for the services to be delivered in accordance with generally accepted industry practice. |
| **Technical Standards:** | The technical standards used as a requirement for this Call-Off Contract are for the services to be delivered in accordance with generally accepted industry practice. |
| **Service level agreement:** | The service level agreement for this Call-Off Contract is as set out in the Supplier’s Service Definition and Service Description. |
| **Onboarding** | The onboarding plan for this Call-Off Contract is as per below:   * Supplier will identify SC cleared resources and provide Buyer with proof of SC clearance. * Buyer will transfer SC clearance from previous department to Buyer. * Upon successful transferal of SC Clearance to the Buyer, the Buyer shall request user accounts and equipment to enable the Supplier to fulfil the scope of work as specified in **Schedule 1 Services.** * Buyer will provide the Supplier with user account details and equipment aligned to the Buyer’s onboarding process. * Supplier will complete any required onboarding processes in the Buyer environment, for example Security Training. |

|  |  |
| --- | --- |
| **Offboarding** | The offboarding plan for this Call-Off Contract is as per below:   * Supplier will notify the Buyer in writing of the roll off dates of the Supplier resources. * Buyer will offboard the Supplier resource account aligned to the roll off date, including any administrative accounts provided. * Buyer will confirm to the Supplier that the Supplier resources have been offboarded. * Supplier will return Buyer equipment. * Buyer will confirm to the Supplier receipt of the Buyer equipment being returned. |
| **Collaboration agreement** | N/A |
| **Limit on Parties’ liability** | Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed 150% per year.  The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed 150% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.  The annual total liability of the Supplier for all other Defaults will not exceed 150% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. |
| **Insurance** | The Supplier insurance(s) required will be:   * a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract] * professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) * employers' liability insurance with a minimum limit of   £5,000,000 or any higher minimum limit required by Law |
| **Buyer’s responsibilities** | The Buyer acknowledges that in order for Supplier to perform the scope of work it will require the Buyer to collaborate with Supplier and execute certain actions under its control. These responsibilities include, but are not limited to, undertaking the following activities:   * Provide access to and input of Buyer subject matter experts (i.e., Buyer system or business processes or user representatives etc.), and/or relevant documentation or other materials in a timely manner. * Directly manage all other non-Supplier managed Buyer third party product or service providers, and such third parties’ dependencies or critical activities. * To provide a single Point of Contact (POC) who will liaise with project team. This single POC will help in:   + Resolving environment related queries   + Resolving functional queries   + Identification of content owners   + Perform any desired UAT   + Provide sign off for the M365 Solution (including amendments)   + Provide sign off for Deliverables   + Knowledge Transfer * Provide the Microsoft 365 / Azure tenant & Google Tenant, along with the required licences. * To provide all project related infrastructure, network, and software including licences with required versions (including third party tools); the cost of licenses will be borne out of Buyer. * Provide test devices matching those in production to allow Microsoft 365 testing. In the event remote working is still required, the client will securely send these devices to supplier so testing can be completed. * Ensure that regulatory requirements and timelines are clear and that regulatory bodies are engaged in a timely manner to ensure that project dependencies can be managed. * Clarifying the differences in policies between source and target. * Installation of M365 Apps on the target computers including Outlook, OneDrive & Teams. * Perform UAT and provide approval to move into Pilot within 2 days of UAT finishing. * Perform data separation, cleansing or remediation. * Migration or creation of user identities. * Provide access to ticketing system for Level 2 migration support. * Contact Microsoft Technical Account Manager and obtain approval to remove throttling limits for migration, if necessary * Ensure stable and functional network connectivity exists between source and target environments and tooling. * Manage updates, changes or handling issues in end user’s devices or any other LOB applications/interfaces impacted by the changes executed. * Manage end user requests or issues through its own L1 Support team. Only Buyer L1 support team will raise L2 support tickets with Supplier L2 support team. All tickets raised with Supplier L2 support team must be appropriately prioritised by the Project team. It is not expected that Supplier staff interact directly with Buyer users for the resolution of issues. * Ensure business approvals for all migrations in place in line with migration and project plan. * Perform remediation’s (including third party tools) and internal project dependencies which may prevent the execution of the services in scope, for example open firewalls ports. Supplier will identify any such issues and provide guidance on how best to address. * Provide fast turnaround time (no later than 3 working days) on critical decisions including, essential information and business approvals which are required to continue with work in progress, or which is critical to meeting a deliverable due date. * Supplier and Buyer will collaborate on mapping, with Buyer providing mapping principles based on the requirements of target architecture, in order to create the migration schedule. * Decommissioning products and environments no longer in use. * Joiners, Movers & Leavers is the responsibility of the Buyer. Joiners should be onboarded directly to the target environment. Leavers should be offboarded in the source environment and removed from the migration scope. |
| **Buyer’s equipment** | The Buyer’s equipment to be used with this Call-Off Contract includes source and target laptops.  Use of the source laptop is required to access the source tenant to validate the discovery data to assist in the migration planning and design. This will involve logging into the source tenant to complete the scope of work as specified in **Schedule 1 Services.**  Use of the target laptop is required to access the target tenant to complete the scope of work as specified in **Schedule 1 Services.** This includes but not limited to execution of test cases, migration, post migration validation and post migration support. |

### Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners** | N/A |

### Call-Off Contract charges and payment

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

|  |  |
| --- | --- |
| **Payment method** | The payment method for this Call-Off Contract is BACS upon receipt of a valid invoice. |
| **Payment profile** | The payment profile for this Call-Off Contract is monthlyin arrears. |
| **Invoice details** | The Buyer will pay the Supplier when the Supplier has submitted their invoice with a valid purchase order to [finance@uksbs.co.uk](mailto:finance@uksbs.co.uk) and [beis.digitalfinance@beis.gov.uk](mailto:beis.digitalfinance@beis.gov.uk) |
| **Who and where to send invoices to** | Invoices will be sent to [finance@uksbs.co.uk](mailto:finance@uksbs.co.uk) and [beis.digitalfinance@beis.gov.uk](mailto:beis.digitalfinance@beis.gov.uk) |
| **Invoice information required** | All invoices must include a valid purchase order number and reference: Con\_5138 |
| **Invoice frequency** | Invoice will be sent to the Buyer monthly in arrears |
| **Call-Off Contract value** | The total value of this Call-Off Contract is £948,130 (exc. VAT). |
| **Call-Off Contract charges** | The breakdown of the Charges is**:**   * Project delivery £920,500 (exc. VAT) * BitTitan migration tooling £27,630 (exc. VAT)   A full breakdown of the call-off contract charges is detailed below in **Schedule 2: Call-Off Contract charges** |

### Additional Buyer terms

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Performance of the** **Service** | This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:  The Supplier has built the migration plan based on experience of migrating over 285,000 M365 users within the past three years, leveraging lessons learnt and accelerators to ensure we align with the Department's desire to start on 20 October 2023 and complete the migration by the end of March 2024, and the assignment can be staffed until the end of 31 March 2025 as required. We will outline each migration stage, including the critical path and milestones.  **Project Duration**  The project key dates are outlined below:   |  |  | | --- | --- | | Project Phase | Date | | Project Start | 20th October 2023 | | Start-Up Phase | 20th October 2023 – 3rd November 2023 | | DCMS to DSIT \* (Google to M365 Migration) | 6th November 2023 – 29th March 2024 | | Live Data Migration Complete | 16th February 2024 | | Archive Migration | 19th February – 15th March 2024 | | Archive Migration Complete | 15th March 2024 | | Verification, Tooling Decommissioning and Project Close | 18th March – 29th March 2024 | | Project Complete | 29th March 2024 |   These phases are also outlined below within the high-level timeline.    **Pre-Start-Up**  With the contract signature mid-October (subject to change), the Pre-Start-Up Plan commences immediately. The Delivery Lead and M365 Technical Lead will work closely with you and your suppliers during this phase. The Delivery Lead will be responsible for the non-technical elements of Start-Up activities, such as resourcing onboarding, whilst the Technical M365 Lead will be responsible for the technical aspects of Start-Up activities, such as provisioning infrastructure and access.  The Pre-Start-Up plan structure is based on our experience delivering similar Google Workspace to M365 migrations. In this phase, we will help you prepare your environment and team for the subsequent stages of work. The Supplier will provide resourcing information, RBAC roles and security clearance proof for the resources engaging in the project. The second part of the Pre-Start-Up phase ensures success with the existing suppliers, integration with early life support, and understanding your standard operating procedures.  **Discovery and Design**  Once the Pre-Start-Up phase is complete, the additional Supplier resources will be onboarded to start working on the Discovery and Design phase. The Supplier will utilise its migration assets to produce tailored readiness reports with inventory assessments, an M365 Migration Approach, and a Migration plan for you.  **Discovery and Design Critical Path**  The critical path for the Discovery phase is:  1. Validating the Discovery and volumetrics provided by DSIT.  2. Installing the Migration tooling software and deployment.  3. Conducting the target state workshops and Migration approach workshops.  **Milestones and Work Products**  1. Google Workspaces to Microsoft 365 Migration Approach  2. Migration Timeline  With our recommended approach to Discovery that follows the Suppliers Delivery Framework, the Departments will benefit from a process that has been successful in many other engagements and can be confident that the Supplier and its consultants will deliver excellence.  **Implementation**  Following Discovery and Design completion, the implementation phase will begin. Test strategy and plans are created, and the remainder of the Suppliers migration team is onboarded. Based on our experience delivering similar migrations and supporting a positive employee experience, early life support is provided during each migration wave.  **Critical Path**  The critical path for the implementation phase is:  1. Mapping migration of source workloads to target workloads.  2. For each workstream, completing a successful migration test and pilot and confirming the waves migrate data positively.  3. Completion of production and archive migration waves, including verification of migrated data.  4. Providing early life support to resolve issues post-implementation.  **Milestones and Work Products**  1. Google Workspaces Test Strategy & Test Cases  2. Project Closure Report |
| **Guarantee** | N/A |
| **Warranties, representations** | N/A |
| **Supplemental requirements in addition to the Call-Off** **terms** | N/A |
| **Alternative clauses** | N/A |
| **Buyer specific**  **amendments**  **to/refinements of the Call-Off Contract terms** | N/A |
| **Personal Data and** **Data Subjects** | Schedule 7 is being used: Annex 1  Subprocessors and other provisions relating to personal data are covered in Schedule 7: Annex 1 |
| **Intellectual Property** | N/A |
| **Social Value** | 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 RM1557.13.

2.2 The Buyer provided an Order Form for Services to the Supplier.

|  |  |  |
| --- | --- | --- |
| **Signed** | Supplier | Buyer |
| **Name** |  |  |
| **Title** |  |  |
| **Signature** |  |  |
| **Date** |  |  |

## Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

[G-Cloud 13 Customer Benefit Record](https://crowncommercial.qualtrics.com/jfe/form/SV_9YO5ox0tT0ofQ0u)

# 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 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 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:

* 2.3 (Warranties and representations)
* 4.1 to 4.6 (Liability)
* 4.10 to 4.11 (IR35)
* 10 (Force majeure)
* 5.3 (Continuing rights)
* 5.4 to 5.6 (Change of control)
* 5.7 (Fraud)
* 5.8 (Notice of fraud)
* 7 (Transparency and Audit)
* 8.3 (Order of precedence)
* 11 (Relationship)
* 14 (Entire agreement)
* 15 (Law and jurisdiction)
* 16 (Legislative change)
* 17 (Bribery and corruption)
* 18 (Freedom of Information Act)
* 19 (Promoting tax compliance)
* 20 (Official Secrets Act)
* 21 (Transfer and subcontracting)
* 23 (Complaints handling and resolution)
* 24 (Conflicts of interest and ethical walls)
* 25 (Publicity and branding)
* 26 (Equality and diversity)
* 28 (Data protection)
* 31 (Severability)
* 32 and 33 (Managing disputes and Mediation)
* 34 (Confidentiality)
* 35 (Waiver and cumulative remedies)
* 36 (Corporate Social Responsibility)
* paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

* + 1. a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’
    2. a reference to ‘CCS’ or to ‘CCS and/or the Buyer’ will be a reference to ‘the Buyer’
    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
  1. The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (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. The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause ‘XX’, where ‘XX’ is the Framework Agreement clause number.
  3. 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 14digit 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 their 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 invoices under the Late Payment of Commercial Debts (Interest) Act 1998.

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

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

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

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

### 9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

9.8.1 premiums, which it will pay promptly

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

### 10. Confidentiality

10.1 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 incorporated Framework Agreement clause

34. 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 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party

shall acquire any right, title or interest in or to the Intellectual Property Rights (“IPR”s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer’s or its relevant licensor’s Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer’s written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier’s or its relevant licensor’s IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

1. alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
2. alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
3. arising from the Supplier’s use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer’s obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier’s breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer 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:

* + 1. rights granted to the Buyer under this Call-Off Contract
    2. Supplier’s performance of the Services
    3. use by the Buyer of the Services

11.7 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:

* + 1. modify the relevant part of the Services without reducing its functionality or performance
    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
    3. buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

* + 1. the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract
    2. other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, 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.npsa.gov.uk/content/adopt-risk-management-approach](https://www.cpni.gov.uk/content/adopt-risk-management-approach) and Protection of Sensitive Information and Assets: <https://www.npsa.gov.uk/sensitive-information-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/technologycode-of-practice/technology -code-of-practice](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/technologycode-of-practice/technology -code-of-practice](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[.](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)

### 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. 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 are reasonable compensation and cover all the Supplier’s avoidable costs or Losses

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

### 19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

* 7 (Payment, VAT and Call-Off Contract charges)
* 8 (Recovery of sums due and right of set-off)
* 9 (Insurance)
* 10 (Confidentiality)
* 11 (Intellectual property rights)
* 12 (Protection of information)
* 13 (Buyer data)
* 19 (Consequences of suspension, ending and expiry)
* 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),

24 (Conflicts of interest and ethical walls), 35 (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:

* + 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
    2. return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
    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
    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
    5. work with the Buyer on any ongoing work
    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
  1. 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.
  2. 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 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 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 take the Term beyond 36 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 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 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the

Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the

Buyer’s liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier’s liability under Clause 24.1 any items specified in Clause

24.2 will not be taken into consideration.

### 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

1. 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

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.

* 1. 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.
  2. 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.
  3. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
     1. its failure to comply with the provisions of this clause
     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
  4. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
  5. 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, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are

reproduced in this Call-Off Contract document at Schedule 7.

# Schedule 1: Services

**Service Description**

**Overview**

Mergers, Acquisitions, Divestitures and Carve-outs (M.A.D. & C.) are becoming more and more common with the race to evolve organisational strategies and become more effective. Although each of M.A.D. & C. has its own unique challenges, and many organisations must go through a similar journey. As part of the journey, organisations have the following high-level business goals:

*Mergers:*

* Combine business entities and operate as a new business entity
* Realise cost savings by reducing redundancies
* Establish a new, unified brand for the new business entity

*Acquisition*

* Integrate an acquired business entity, asset or capability into the existing business entity
* Realise cost savings by reducing redundancies
* Promote brand of existing business entity (the acquiring entity)

*Divestiture & Carve-Outs*

* Separate a divested business entity, asset or capability from the existing business entity
* Form divesture through acquisition by another existing business entity or itself becoming a new business entity
* Cease usage of existing business entity brand (the divesting entity) by divesture

Supplier’s approach to M.A.D. & C. projects has been evolving over the past few years, and we are focused on supporting business transformation, technical delivery, and organizational change management activities. Supplier provides the following services for its clients who are embarking or has already embarked on their M.A.D. & C. projects:

* Advisory services to identify areas which would impact the end-to-end user experience, the present risk to a successful organizational transformation or gaps which may be a result of the nature of M.A.D. & C. (e.g., security policies between the two organisations)
* Detailed planning and implementation services to ensure the business goals are supported by the correct technology and tools underpinned by the experience of Supplier which has delivered similar projects globally
* Migration services to ensure structured or unstructured data is moved between the organisations in a secure and reliable way. The migration services cover email migrations, file server to SharePoint Online / OneDrive migrations, Teams migrations, SharePoint Server to SharePoint Online services or other M365 and D365 workload migrations depending on the client environment.
* Employee experience is driven by Viva Insights to help the new organizational behaviour and culture evolve in a way that will empower the employees to become more effective and collaborate with other employees and customers to realise the benefits of the transition and transformation.

**Scope of Work**  
*Scope Volumetrics*

The scope volumetrics below was used by the Supplier to base this Service upon.

|  |  |  |
| --- | --- | --- |
| Department | Migration | High Level Scope |
| DSIT | DCMS to DSIT \*  (Google to M365 migration)  \*DSIT is taking over former BEIS tenancy which it shares with DESNZ. | * 1800+mailboxes, * 1800+ personal drives, * 155 shared Google Drives (4.5 TB) * 1.3 AO Docs files |

The Supplier will perform the services, as outlined in the below, for the Buyer:

*Project Management*

* Create the Project plan in conjunction with the Buyer Project Manager.
* Maintain the Project plan in conjunction with the Buyer Project Manager.
* Manage the Supplier activities in the Project plan.
* Track the Deliverables status against the Project plan.
* Manage the Supplier Project resources for the duration of the Project.
* Prepare for and attend the Project Governance meetings as outlined in Governance section.
* Measure the Project’s performance and regularly report status to Buyer Project Manager.
* Collaborate with Buyers existing suppliers to deliver the agreed outcomes of this project

*Discovery and Design*

Perform a review of the source tenant with a view to creating a final migration inventory to validate the migration volumetrics for the source tenant and create a migration strategy.

The following activities will be carried out.

* Tenant Design review for source and target M365 and Google Tenants
* Tools & Scripts: Validate discovery data from the source tenants to discover (Google Mailboxes, Google Drives (Personal and Shared), Google Vault & AO Docs).
  + BitTitan and PowerShell Scripts are the intended tools to be used on the project.
  + Provide discovered volumetrics from the source tenants that includes a final inventory to be migrated for agreement with the client
* Workshop: Perform Up to 5 x 2-hour workshops (Google Mailboxes, Google Drives (Personal and Shared), Google Vault & AO Docs) to define the target state and identify critical dependencies across M365 and Google Apps
* Workshop: Perform 5 x 3-hour workshops (Google Mailboxes, Google Drives (Personal and Shared), Google Vault & AO Docs) for defining the migration approach for all Google Apps to M365.
* Documentation: Document the migration approach final scope, migration architecture, and successful migration measure for each workload
* Documentation: Create a migration plan – timelines and waves
* Determine the pilot and production migration scope to validate migration approach and throughput
* Create migration plan and schedule with the Buyers Migration Team

*Build, Test and Pilot*

Build

* Build and Configure Migration Tooling
  + BitTitan
    - Google Mailboxes, calendar and contact to M365
    - Google Vault to M365
    - Google Drives (Shared) to M365
    - Google Drives (Personal) to M365

Test

* Creation of Test Plan and Test Scripts
* Execute SIT testing and complete Test Scripts
* Validate migration throughput.

Pilot

* Pilot up to 50 Users for Mail and OneDrive and up to 5 SharePoint and Teams sites
* Create Source and target Mappings for Pilot migrations based on client supplied mapping files.
* Execute and Test Pilot Migration jobs (Make changes to the migration approach as required based on the pilot results)

*Deploy & Hypercare*

Deploy

* Create Source to Target migration mapping file - The Supplier will be provided with a requirement for each individual migration. The requirement will cover:
  + The source and target content locations. E.g., the MS Team, SharePoint site etc.
  + Where the source content needs to be split and distributed between several locations, the requirement will state this at the highest practical level. E.g., library or folder level
  + It will be the responsibility of the Migration Service Provider to identify the full set of content to be migrated within the scope of the requirement. E.g., all items in a Team, site, folder etc.
* Pre-seed of content from source to target tenant
* Execute Migration according to agreed migration schedule by performing a final delta sync and cutover for the following in scope applications - Google Mailboxes, Google Drives (Personal and Shared), Google Vault & AO Docs
  + Some migrations will execute overnight and be ready for hand over to the business the next day while others will be transferred during the working day.
* Migration Verification and Reporting
  + After each individual migration, the Migration Service Provider will supply the Importing Department with a report demonstrating that every version of every item has been successfully migrated, along with a summarized view of this.
  + The Migration Service Provider shall use their tool and their checks to correct for any assets that were not correctly migrated.

**Hypercare**

* Migration issues investigation and resolution up to 3 days per migrated object, after which support will become the responsibility of the Buyer.
* Where the migration has failed the service provider will attempt to remigrate those in the same day. If these still are not migrated, the root cause will be investigated, and the migration will be rescheduled for one further attempt. If migrations still fail, the issue will be raised to the project and Buyer team leadership to agree on a plan for troubleshooting and fixing the underlying root cause.
* Provide Knowledge Transfer to Support Teams via 2 workshops up to 2 hours each.

**Work Products**

Supplier will deliver to the Buyer the Work Products listed below:

|  |  |  |  |
| --- | --- | --- | --- |
| # | Work Product Title | Work Product Description | Format |
| WP01 | Google Migration to M365 Migration Design and Approach | Google Migration Design and Approach, including:   * Migration Approach for Google Mail & Google Drives (Personal & Shared) * Migration Scope, Risks, Assumptions & Dependencies * Migration team Roles & Responsibilities * Security Consent and Account permissions * Migration Tools & Infrastructure * Roll back * Detailed Migration Design by Phases – * Preparation & Configuration, * Assessment * Execution (prepare source and target environment, \*Migration validation and \* Cutover) | Microsoft  Word |
| WP02 | Google to M365 Migration Timeline | Document per workload detailing the Migration timelines and waves.  Including:   * Migration scope and migration times * Testing criteria * Migration Waves plan | Microsoft Excel / Microsoft Project |
| WP03 | Google to M365 Migration Test Strategy & Test Cases | A test plan and test cases used to test the end-to-end solution.   * Google Mail * Google Drives (Personal & Shared) | Microsoft Excel |
| WP04 | Google to M365 Migration (DCMS to DSIT) Closure Report | Document detailing open issues at the end of the migration, including.   * Introduction * Migration Solution Overview * Test approach and completion results * Migration results * Open Issues at the end of the migration | Microsoft Word |

Work Products do not require formal Buyer reviews and approvals

**Governance**

The parties acknowledge the undertaking of the Project involves collaboration and coordination pursuant to the governance forums set out below:

|  |  |  |  |
| --- | --- | --- | --- |
| Forum Title | Objective | Participants | Periodic Frequency and Estimated Duration |
| Daily Checkpoint | A daily virtual checkpoint to assess:   * Project activities completed since the last meeting * Project activities to be completed by the next meeting * Impediments to Project progress and make decisions to remove barriers * Migration status reporting, including, number of users migrated, and number of failures / errors encountered. | Supplier:   * Delivery Lead * Technical Architect   Buyer:   * Project Manager   Team members with open actions will attend, attendee list will vary as Project progresses, but meeting will be fixed. | Daily, 30 minutes |
| Weekly Project Status Meeting | A weekly checkpoint to assess Project status and coordinate Project activities, review and make decisions regarding Project risks, issues, actions, dependencies and change requests, as well as:   * Activities completed this week * Activities planned, but not completed, this week * Activities to be completed next week * Impediments to progress and make decisions to remove barriers | Supplier:   * Delivery Lead * Technical Architect   Buyer:   * Project Manager   Other Buyer attendees, as required. | Weekly, one hour |
| Project Steering Board (Operational Board) | To provide guidance and make strategic decisions, resolve escalations and provide oversight throughout the Project duration. | Supplier:   * Delivery Lead   Buyer:   * Programme Manager * Project Manager   Other Buyer attendees, as required. | Monthly, one hour |

**Assumptions**

* We expect to maintain a continuous and consistent following throughput as outlined below:
  + Exchange Online - Throughput of 40 GB per hour.
  + SharePoint Online. Throughput of 10 GB per hour.
  + OneDrive for Business. Throughput of 50 GB per hour.
  + Teams. Assumed throughput of 10 GB per hour.
* Tools, network, Buyer environment and target Office 365 can handle the migrations at the required throughput. Throughput will be evaluated in two dimensions:
  + Technical capability to achieve speed
  + Business ability to cope and drive migrations at that speed
* The volumetrics provided by BEIS are assumed to be accurate. Volumetrics can be found in **Schedule 1 Services.**
* Migration Velocity will be 150 user per day migrating Monday – Thursday.

Where an assumption proves incorrect, Supplier shall not be liable for any failure to meet its obligations under this Order. If the scope of work within this Order is impacted due to an assumption proving incorrect, the Project schedule will be amended by an agreed period arising from the incorrect assumption.

**Implementation Plan**

The project key dates are outlined below:

A screenshot of a computer

Description automatically generated

A white rectangular object with text

Description automatically generated with medium confidence

# Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the

Supplier’s Platform pricing document) can’t be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Supplier's total cost for delivering this project between 20 October 2023 and the end of March 2024, including the migration tooling, is £948,130 (excluding VAT).

If additional activities are required beyond the end of March 2024, during the contract period to end March 2025, these will be agreed upon by the Parties and will be costed on a Time & Materials basis according to the Supplier’s G-Cloud 13 rate card.

**Project delivery**

The table below provides Supplier G-Cloud 13, SFIA, Time and Materials rates that will apply for the applicable Supplier resources providing services chargeable for this project.

| Project Role | SFIA Grade | Location | Estimated Days  (8-hour day) | SFIA Day Rates (GBP) | Fees  (GBP) |
| --- | --- | --- | --- | --- | --- |
| **Project governance and oversight** | | | | | |
| Delivery Lead | 7 | UK | 94 | 2200 | £206,800 |
| Technical Architect | 7 | UK | 33 | 2200 | £72,600 |
| Client Executive | 7 | UK | 9 | 2200 | £19,800 |
| **DCMS to DSIT - (Google to M365 migration)** | | | | | |
| Google Workplaces SME (Mail) | 5 | UK | 57 | 1300 | £74,100 |
| Google Workplaces SME (Google Drives) | 5 | UK | 57 | 1300 | £74,100 |
| Google Workplaces SME (Google Shared Drives) | 6 | UK | 77 | 1850 | £142,450 |
| Migration Lead | 6 | UK | 85 | 1800 | £153,000 |
| Migration Engineer | 4 | UK | 85 | 950 | £80,750 |
| Migration Engineer | 4 | UK | 63 | 950 | £59,850 |
| Migration Engineer | 4 | UK | 39 | 950 | £37,050 |
| **Estimated T&M Cost** | | | | | **£920,500** |

**Tooling**

The estimated additional cost for the proposed migration tooling is detailed below. The cost excludes VAT.

|  |  |
| --- | --- |
| Tooling | Estimated Cost (GBP) |
| BitTitan | £27,630 |
| **Total** | **£27,630** |

**G-Cloud 13 rate card**

Rate Card for calculation of Time and Materials charges

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SFIA Grade and Level | Strategy and architecture | Change and Transformation | Development &  implementation | Relationships & Engagement |
| **1 Follow** | £375 | £375 | £375 | £375 |
| **2 Assist** | £550 | £550 | £500 | £500 |
| **3 Apply** | £800 | £800 | £750 | £750 |
| **4 Enable** | £1050 | £1050 | £950 | £950 |
| **5 Ensure or advise** | £1400 | £1400 | £1300 | £1300 |
| **6 Initiate or influence** | £1850 | £1850 | £1800 | £1800 |
| **7 Set strategy or inspire** | £2200 | £2200 | £2100 | £2100 |

# Schedule 3: Collaboration agreement

Not Used

## Schedule 4: Alternative clauses

### Not Used

## Schedule 5: Guarantee

Not Used

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

|  |  |
| --- | --- |
| **Expression** | **Meaning** |
| **Additional Services** | Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) 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 Platform). |
| **Audit** | An audit carried out under the incorporated Framework Agreement clauses. |
| **Background IPRs** | For each Party, IPRs:   * owned by that Party before the date of this Call-Off Contract   (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes   * created by the Party independently of this Call-Off Contract, or   For the Buyer, Crown Copyright which isn’t available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software. |
| **Buyer** | The contracting authority ordering services as set out in the Order Form. |
| **Buyer Data** | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer. |
| **Buyer Personal Data** | The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract. |
| **Buyer Representative** | The representative appointed by the Buyer under this Call-Off Contract. |

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

|  |  |
| --- | --- |
| **Data Loss Event** | Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach. |
| **Data Protection Impact** **Assessment (DPIA)** | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| **Data Protection** **Legislation (DPL)** | (i) the UK GDPR 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. |
| **Data Subject** | Takes the meaning given in the UK GDPR |
| **Default** | Default is any:   * breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) * other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract   Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer. |
| **DPA 2018** | Data Protection Act 2018. |
| **Employment Regulations** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) (‘TUPE’) . |
| **End** | Means to terminate; and Ended and Ending are construed accordingly. |
| **Environmental**  **Information Regulations or EIR** | The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information  Commissioner or relevant government department about the regulations. |
| **Equipment** | The Supplier’s hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract. |

|  |  |
| --- | --- |
| **ESI Reference Number** | The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool. |
| **Employment Status** **Indicator test tool or ESI tool** | The HMRC Employment Status Indicator test tool. The most up-to date version must be used. At the time of drafting the tool may be found here:  [https://www.gov.uk/guidance/check-employment-status-fortax](https://www.gov.uk/guidance/check-employment-status-for-tax) |
| **Expiry Date** | The expiry date of this Call-Off Contract in the Order Form. |
| **Force Majeure** | A force Majeure event means anything affecting either Party's performance of their obligations arising from any:   * acts, events or omissions beyond the reasonable control of the affected Party * riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare * acts of government, local government or Regulatory Bodies * fire, flood or disaster and any failure or shortage of power or fuel * industrial dispute affecting a third party for which a substitute third party isn’t reasonably available   The following do not constitute a Force Majeure event:   * any industrial dispute about the Supplier, its staff, or failure in the Supplier’s (or a Subcontractor's) supply chain * any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure * the event was foreseeable by the Party seeking to rely on Force   Majeure at the time this Call-Off Contract was entered into   * any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans |
| **Former Supplier** | A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor). |
| **Framework Agreement** | The clauses of framework agreement RM1557.13 together with the Framework Schedules. |
| **Fraud** | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or |

|  |  |
| --- | --- |
|  | defrauding or attempting to defraud or conspiring to defraud the Crown. |
| **Freedom of Information** **Act or FoIA** | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation. |
| **G-Cloud Services** | The cloud services described in Framework Agreement Clause 2 (Services) 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. |
| **UK GDPR** | The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679). |
| **Good Industry Practice** | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |
| **Government**  **Procurement Card** | The government’s preferred method of purchasing and payment for low value goods or services. |
| **Guarantee** | The guarantee described in Schedule 5. |
| **Guidance** | Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence. |
| **Implementation Plan** | The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding. |
| **Indicative test** | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6. |
| **Information** | Has the meaning given under section 84 of the Freedom of Information Act 2000. |

|  |  |
| --- | --- |
| **Information security management system** | The information security management system and process developed by the Supplier in accordance with clause 16.1. |
| **Inside IR35** | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool. |

|  |  |
| --- | --- |
| **Insolvency event** | Can be:   * a voluntary arrangement * a winding-up petition * the appointment of a receiver or administrator * an unresolved statutory demand * a Schedule A1 moratorium * a Dun & Bradstreet rating of 10 or less |
| **Intellectual Property** **Rights or IPR** | Intellectual Property Rights are:   * copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information * applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction * all other rights having equivalent or similar effect in any country or jurisdiction |
| **Intermediary** | For the purposes of the IR35 rules an intermediary can be:   * the supplier's own limited company * a service or a personal service company * a partnership   It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). |
| **IPR claim** | As set out in clause 11.5. |
| **IR35** | IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary. |
| **IR35 assessment** | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35. |

|  |  |
| --- | --- |
| **Know-How** | All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier’s or Buyer’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, 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. |
| **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 Schedule 6. |
| **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 UK GDPR. |
| **Personal Data Breach** | Takes the meaning given in the UK GDPR. |
| **Platform** | The government marketplace where Services are available for Buyers to buy. |
| **Processing** | Takes the meaning given in the UK GDPR. |
| **Processor** | Takes the meaning given in the UK GDPR. |
| **Prohibited act** | To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:   * induce that person to perform improperly a relevant function or activity * reward that person for improper performance of a relevant function or activity * commit any offence:   + under the Bribery Act 2010   + under legislation creating offences concerning Fraud   + at common Law concerning Fraud   + committing or attempting or conspiring to commit Fraud |

|  |  |
| --- | --- |
| **Project Specific IPRs** | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier’s Background IPRs. |
| **Property** | Assets and property including technical infrastructure, IPRs and equipment. |
| **Protective Measures** | Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it. |
| **PSN or Public Services** **Network** | The Public Services Network (PSN) is the government’s high performance network which helps public sector organisations work together, reduce duplication and share resources. |
| **Regulatory body or bodies** | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract. |
| **Relevant person** | Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body. |
| **Relevant Transfer** | A transfer of employment to which the employment regulations applies. |
| **Replacement Services** | Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-  Off Contract, whether those services are provided by the Buyer or a third party. |
| **Replacement supplier** | Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer). |
| **Security management plan** | The Supplier's security management plan developed by the Supplier in accordance with clause 16.1. |

|  |  |
| --- | --- |
| **Services** | The services ordered by the Buyer as set out in the Order Form. |
| **Service data** | Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data. |
| **Service definition(s)** | The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn’t limited to, those items listed in Clause 2 (Services) of the Framework Agreement. |
| **Service description** | The description of the Supplier service offering as published on the Platform. |
| **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-controlsche ck-if-you-need-approval-to-spend-money-on-a-service](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: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

## 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:

1.2 The contact details of the Supplier’s Data Protection Officer are: Richard Steen [avanadepo@avanade.com](mailto:avanadepo@avanade.com)

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

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

|  |  |
| --- | --- |
|  |  |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below:  ***(Note: Customer data in the below instances refer to Buyer users of the Google and M365 platforms).***  **Customer Data:** This is all data, including text, sound, video, or image files and software that the Buyer provides to the Supplier or that is provided on the Buyer’s behalf through their use of Google and Microsoft M365 services. It includes data that customers upload for storage or processing, as well as customizations. Examples of Customer Data processed in Google include email content in Google Mail and documents in Google Drive and in M365 include email content in Exchange Online, and documents or files stored in SharePoint Online or OneDrive for Business.  **Service-generated Data:** This is data that is generated or derived by using the Google and M365 services, such as usage or performance data. Most of this data contains pseudonymous identifiers generated by Google or Microsoft such as unique identifiers (typically a number generated by the system) that cannot on its own identify an individual person but is used to deliver the enterprise services to users.  **Diagnostic Data:** This data is collected or obtained by Google and Microsoft from software that is locally installed by the Buyer in connection with the Online Service and may also be referred to as telemetry. This data is commonly identified by attributes of the locally installed software or the machine that runs that software.  **Support Data:** This is data provided to the Supplier by or on behalf of Buyer (or that Buyer authorises Google or Microsoft to obtain from an Online Service) through an engagement with Google or Microsoft to obtain technical support for Online Services.  Customer Data, System-generated Log Data, and Support Data do not include administrator and billing data, such as Buyer administrator contact information, subscription information, and payment data, which the Supplier will collect and process in its capacity as a data controller. |
| Duration of the Processing | For the duration of the agreement. |
| Nature and purposes of the Processing | The nature of the Processing means the retrieval and collection of all user data by the BitTitan migration tooling with the intention to migrate and copy from the Buyers Google Tenant to the Buyers M365 tenant.  The purpose of Processing relates to the migration of all user data from the Buyers Google tenant to the Buyers M365 tenant to form a single tenancy. |
| Type of Personal Data | Personal data within Google and M365 is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. Personal data within the Google and M365 product application suite can include:   * Name * Home address * Work address * Telephone number * Mobile number * Email address * Passport number * National ID card * Social Security Number (or equivalent) * Driver's license * Physical, physiological, or genetic information * Medical information * Cultural identity * Bank details/account numbers * Tax file number * Work address * Credit/Debit card numbers * Social media posts * IP address (EU region) * Location/GPS data * Cookies   Further details of some of these personal data elements described below:   * User IP address, which is used to access the Google and M365 applications, cookies, connection data and access times. * Username (access data to Google and M365 applications), data within the scope of the so-called multi-factor authentication, which you have stored in your Google and Microsoft account (e.g. optionally your (private) mobile phone number). * Identification features: Information about you that identifies you as a user, sender, recipient of data within Google and M365. This includes in particular the following master data: Surname, first name, contact data including telephone number, e-mail address, office fax number, insofar as this has been provided by you. Further data (such as a profile picture you have stored) can also be viewed in your profile at any time. * Data required for authentication and for the use of the license. In Google and M365, all user activities such as time of access, date, type of access, information about the data/files/documents accessed and all activities in connection with the use, such as creating, changing, deleting a document, setting up a team (and channels in teams), taking notes in the notebook, starting a chat and replying in the chat are processed. * Films, pictures and video and sound recordings. * Metadata used for the maintenance of the service provided. * Any data as (potentially) processed in the context of file sharing for professional activities (e.g. messages, images, files, voicemail, calendar meetings, contacts and the like). * Audit logs: Each operation within the audit logs contain data that can be attributed directly to an identifiable person. The following fields appear in each event:  1. UserType 2. UserKey 3. RecordType 4. Id 5. UserId 6. Version 7. OrganisationId 8. Workload 9. Operation 10. CreationTime 11. ObjectId   The log files can show a directly identifiable person performed an action at a specific time, with which browser and from which operating system.  Microsoft also records whether there was a login error, what the cause was, and how the user was authenticated. The users are directly identifiable by the fields with the user name and the email address. These access files also contain the used IP address.  Because each log line contains the combination of UserId and Organisation ID, each log line is personal data. In addition, these log files contain information about actions on the servers, and content data from names of paths and files.   * Diagnostic Data: MyAnalytics, Workplace Analytics, Office Delve and Activity Reports store detail on all kinds of activities per user, such as email behaviour, use of the email app, Google Drive, Teams and activity in OneDrive and SharePoint Online. * Other events: These occur depending on the type of activity, such as the name of the application used (ApplicationID and ApplicationDisplayName), actions such as editing, viewing, uploading, downloading or renaming a file or folder (FileModified, FilePreviewed, FileAccessed, FileUploaded, FileDownloaded, FileRenamed, FolderCreated, FolderModified), logging in, giving or withdrawing sharing permissions, adding to a group, or creating a list. * These events contain additional unique identifiers, such as ClientIP and CorrelationID, and content information, such as SiteURL, SourceFileName, WebID, and SourceRelativeUrl. |
| Categories of Data Subject | Staff  Other Government Department staff  Suppliers  Customers/Clients  Members of the public |
| 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 | This will not be applicable, because at the end of the contract all data will reside in the Buyer’s environment.  Data will only be held until copy deltas have been successfully verified during the migration process and will be periodically destroyed during this period: October 2023- March 2025.  All data will be destroyed on decommissioning of the migration tools and completion of the project anticipated March 2025. |

## Annex 2: Joint Controller Agreement

### **NOT USED**

### 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 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (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 [select: Supplier or Buyer]:

1. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
2. 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;
3. is solely responsible for the Parties’ compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
4. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
5. 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 [select: Supplier’s or 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:

1. report to the other Party every [insert number] months on:
   * 1. the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
     2. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
     3. 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;
     4. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
     5. 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;
2. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
3. 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;
4. 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;
5. request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
6. 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;
7. 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:
   * + 1. are aware of and comply with their ’s duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information
       2. 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;
       3. have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;
8. ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
9. nature of the data to be protected;
   * + 1. harm that might result from a Data Loss Event;
       2. state of technological development; and
       3. 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 it 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:

1. 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; and
2. all reasonable assistance, including:
   * 1. 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;
     2. 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;
     3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
     4. 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:

1. the nature of the Personal Data Breach;
2. the nature of Personal Data affected;
3. the categories and number of Data Subjects concerned;
4. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
5. measures taken or proposed to be taken to address the Personal Data Breach; and
6. describe the likely consequences of the Personal Data Breach.

### 4. Audit

4.1 The Supplier shall permit:

1. 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
2. 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 UK 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:

1. 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
2. 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 UK 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:

1. 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;

1. 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
2. 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 clause 32 of the Framework Agreement (Managing disputes).

* 1. 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.
  2. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):

1. if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;
2. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
3. 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. Termination

8.1 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 5.1.

### 9. Sub-Processing

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

1. 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
2. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

### 10. Data Retention

10.1 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 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.