



**Crown
Commercial
Service**

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

Between

The Secretary of State for the Department for Education

And

Kainos Worksmart Ltd

For

Workday Implementation Services (HR, Payroll & Expenses)

Contents

| | |
|---|-------------------------------------|
| G-Cloud 11 Call-Off Contract (version 4) | 1 |
| Part A - Order Form | 4 |
| Principle contact details | 5 |
| Call-Off Contract term..... | 5 |
| Buyer contractual details..... | 6 |
| Supplier's information | 10 |
| Call-Off Contract charges and payment | 10 |
| Additional Buyer terms..... | 11 |
| Schedule 1 - Services | Error! Bookmark not defined. |
| Schedule 2 - Call-Off Contract charges | Error! Bookmark not defined. |
| Part B - Terms and conditions | Error! Bookmark not defined. |
| 1. Call-Off Contract start date and length..... | 16 |
| 2. Incorporation of terms | 17 |
| 3. Supply of services..... | 18 |
| 4. Supplier staff | 19 |
| 5. Due diligence | 20 |
| 6. Business continuity and disaster recovery | 20 |
| 7. Payment, VAT and Call-Off Contract charges..... | 21 |
| 8. Recovery of sums due and right of set-off | 22 |
| 9. Insurance | 22 |
| 10. Confidentiality..... | 24 |
| 11. Intellectual Property Rights | 24 |
| 12. Protection of information..... | 26 |
| 13. Buyer data | 26 |
| 14. Standards and quality | 28 |

| | |
|--|-----------|
| 15. Open source | 29 |
| 16. Security | 29 |
| 17. Guarantee | 30 |
| 18. Ending the Call-Off Contract..... | 30 |
| 19. Consequences of suspension, ending and expiry | 32 |
| 20. Notices..... | 33 |
| 21. Exit plan | 34 |
| 22. Handover to replacement supplier | 35 |
| 23. Force majeure..... | 36 |
| 24. Liability..... | 36 |
| 25. Premises..... | 37 |
| 26. Equipment | 38 |
| 27. The Contracts (Rights of Third Parties) Act 1999 | 38 |
| 28. Environmental requirements | 38 |
| 29. The Employment Regulations (TUPE)..... | 39 |
| 30. Additional G-Cloud services..... | 41 |
| 31. Collaboration | 41 |
| 32. Variation process | 41 |
| 33. Data Protection Legislation (GDPR) | 42 |
| Schedule 3 – Not Used | 42 |
| Schedule 4 – Not Used Alternative clauses | 42 |
| Schedule 5 – Not Used | 42 |
| Schedule 6 - Glossary and interpretations | 42 |
| Schedule 7 - GDPR Information..... | 52 |
| Annex 1 - Processing Personal Data | 52 |

Part A - Order Form

| | |
|---|---|
| Digital Marketplace service ID number: | 357314460582574 |
| Call-Off Contract reference: | PROJ_4876 Supplier Reference: SO013577 |
| Call-Off Contract title: | Workday Application Management Services (AMS) |
| Call-Off Contract description: | The Supplier has been engaged by the Buyer to provide Workday AMS |
| Start date: | On signature of contract |
| Expiry date: | 31 March 2021 |
| Call-Off Contract value: | Up to £78,000 ex VAT |
| Charging method: | Invoice/Bank Transfer |
| Purchase order number: | TBC |

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

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

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

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

| | |
|------------------------|---|
| From: the Buyer | THE SECRETARY OF STATE FOR EDUCATION whose Head Office is at Sanctuary Buildings, Great Smith Street, London, SW1P 3BT; |
|------------------------|---|

| | |
|-------------------------|---|
| To: the Supplier | Kainos WorkSmart Limited 02890 571100 Supplier's address: Kainos House, 4-6 Upper Crescent, Belfast, BT7 1NT Northern Ireland Company number: NI622516 |
| Together: the 'Parties' | |

Principle contact details

| | |
|-------------------|------------|
| For the Buyer: | <REDACTED> |
| For the Supplier: | <REDACTED> |

Call-Off Contract term

| | |
|------------------------------|---|
| Start date: | This Call-Off Contract starts on the date of signature and is valid until 31 March 2021. Subject to additional internal approvals it can be extended for a period of a further 6 months in accordance with the extension period below. |
| Ending (termination): | The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause. |
| Extension period: | <p>This Call-Off Contract can be extended by the Buyer for 1 period of up to 6 months each by giving the Supplier 1 month's written notice before its expiry.</p> <p>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p> <p>The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.</p> <p>Under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS) if the:</p> <ul style="list-style-type: none"> • Buyer is a central government department • contract Term is intended to exceed 24 months |

Buyer contractual details

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

| G-Cloud lot: | This Call-Off Contract is for the provision of Services under: Lot 3 - Cloud Support | | | | |
|----------------------------|---|------------------------|----------------------|------------------------|----------------------|
| G-Cloud services required: | The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: Service ID: 357314460582574 – link below “Gcloud listing” GCloud listing | | | | |
| Additional Services: | N/A | | | | |
| Location: | The Services will be delivered remotely. | | | | |
| Quality standards: | The Supplier warrants that it will carry out the services with reasonable care and skill and that all services supplied hereunder shall be of satisfactory quality and fit for the particular purpose for which they are supplied with reference to the Customer's requirements and in line with G-Cloud 11 offerings The Supplier must confirm to the ISO 9001:2008 Quality Management System The quality standards specified within Service Requirements description outlined in Framework Section 2 will also apply. | | | | |
| Technical standards: | The technical standards required for this Call Off contract are: i) System security, availability and reliability maintained to ISO270001/20000-1/22301/27018 standards ii) Tool to remain compatible with current Microsoft software and Internet Browsers iii) Cyber Essentials accreditation Compliance with accessibility standards W3C WA1: WCAG 2.0 AA level | | | | |
| Service level agreement: | The following Target Response Times and Incident Classifications apply to the provision of the Services: <table><tr><th>Priority</th><th>Classification</th><th>Description & Examples</th><th>Target Response Time</th></tr></table> | Priority | Classification | Description & Examples | Target Response Time |
| Priority | Classification | Description & Examples | Target Response Time | | |

| | | | | |
|--|-----------------|---|---|---------|
| | Critical | High Impact & High Urgency | Business critical integration or software functionality not usable for any purpose; Data inaccuracies impacting all Workday users; All users affected; Unable to proceed and creating major business impact. | 1 hour |
| | High | High Impact & Medium Urgency; Medium Impact & High Urgency | Malfunction impacting important integration or software functionality; Business process, absence plan, benefits plan or similar isn't completing; Majority of users affected. | 2 hours |
| | Medium | High Impact & Low Urgency; Medium Impact & Medium Urgency Low Impact & High Urgency | Malfunction impacting standard integration or software functionality; Business process, absence plan, benefits plan or similar creating an issue, but workaround available; Multiple users affected. | 4 hours |
| | Low | Medium Impact & Low Urgency Low Impact & Medium Urgency | Malfunction impacting non-critical integration or software functionality; Business process, absence plan, benefits plan or similar requires amending, but not blocking progress; Single user affected or multiple users | 1 day |

| | | | | |
|---------------------|---|---|---|--------|
| | | | inconvenienced. | |
| | Minor | Low Impact & Low Urgency | Minor issue inconveniencing users; No impact on business; Cosmetic modification; Usability suggestion. | 2 days |
| | Query | Request for advice, guidance or information | Request for investigation into behaviour of functionality; Request for instructions or guidance on how to achieve outcome. | 2 days |
| | Service Request | Standard change that does not require approval | Password reset; Set up of new incident management application user. | 2 days |
| | Problem | Investigation of underlying root cause of 1 or more Incidents | Grouping of one or more Incidents with similar symptoms to investigate and resolve underlying root cause. | 2 days |
| | Change Request | Request for change or enhancement | Introduction of new functionality; Enhancement of existing functionality. | 2 days |
| Onboarding: | There is no requirement for on-boarding activity as the buyer is already set up on the Suppliers KIM system. | | | |
| Offboarding: | <p>The off-boarding plan for this Call-Off Contract will be developed by the Supplier and agreed between the Buyer and the Supplier within 4 weeks of the contract commencement date and reviewed 4 weeks prior to the end of the contract. As a minimum this will involve:</p> <ul style="list-style-type: none"> Ensuring the transfer of knowledge to the Buyer, a representative nominated by the Buyer or a different | | | |

| | |
|-------------------------------------|--|
| | <p>Supplier,</p> <ul style="list-style-type: none"> Ensuring the return of any Data within agreed deadlines <p>It is acknowledged and agreed that whilst the Supplier will work with the Buyer and provide all reasonable opportunities to facilitate knowledge transfer, the Supplier is not representing or warranting that after the knowledge transfer the Buyer staff will be able to assume all aspects of the service in house as this will be contingent on, without limitation, the background of the Buyer staff and their level of participation.</p> <p>Any offboarding requested by the Buyer, had not been included within the estimated costs and will be provided by the Supplier, at the G-Cloud rates, and charged on a time and materials basis.</p> |
| Collaboration agreement: | Not applicable although it is recognised that the Supplier, in order to deliver the service, needs to collaborate and work in partnership with Workday the HR, Payroll and Expenses solution Provider. |
| Limit on Parties' liability: | <p>The annual total liability of either Party for all Property defaults will not exceed £1,000,000</p> <p>The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term</p> <p>The annual total liability for all other defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> |
| Insurance: | <p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G- Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law |
| Force majeure: | A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days |
| Audit: | <p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits.</p> <p>7.4</p> <p>7.5</p> <p>7.6</p> <p>7.7</p> <p>7.8</p> |

| | |
|----------------------------------|---|
| | 7.9 7.10 7.11 7.12 7.13 |
| Buyer's responsibilities: | The Buyer is responsible for the tasks outlined in the assumptions and dependencies sections above, the Supplier Workday Implementation Methodology and the Supplier's terms and conditions on the Digital Marketplace. |
| Buyer's equipment: | The Buyer's equipment to be used with this Call-Off Contract includes N/A |


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 |
| Payment profile: | Pre-Paid Hours (to include Pre-Paid Service Management Hours) are invoiced quarterly in advance. Additional Hours, On-Call Support, Customer Requested Overtime and/or Expenses (where applicable) are invoiced monthly in arrears based on the previous month's usage. Payment terms are thirty (30) days net (Due Date). |
| Invoice details: | As above. |
| Who and where to send invoices to: | <REDACTED> |
| Invoice information required – for example purchase order, project reference: | <p>A valid invoice is one that is:</p> <ul style="list-style-type: none"> • Is in an un-editable format such as pdf or jpeg • Delivered in timing in accordance of the contract and is not future dated • Is for the correct sum • Is correct in terms of services/goods supplied • Has a unique invoice number • Quotes a valid Purchase Order number • Includes correct supplier details, date, contact details • Valid Contract Number |

| | |
|-----------------------------------|---|
| | <ul style="list-style-type: none"> • Invoicing will be in £ Sterling • A copy invoice shall simultaneously be emailed to the DfE Buyer and the central mailbox Budgets.HRGrp@education.gov.uk to enable the Buyer to take receipting action |
| Invoice frequency: | Quarterly in advance for Pre-Paid hours. Monthly in arrears for all other services, based on actual usage. |
| Call-Off Contract value: | The total value of this Call-Off Contract: The Buyer's budget is up to £78,000 ex VAT |
| Call-Off Contract charges: | <p>The breakdown of the Charges is as set out below, the Charges are estimates and have been compiled based on the assumptions and dependencies set out G-Cloud services required' section above:</p> <p><REDACTED></p> <p>Service performance and deliverables will be agreed, documented, and reviewed at monthly AMS review meetings against the SLAs stated above.</p> <div style="text-align: center;">  <p>Kainos Pricing</p> </div> |

Additional Buyer terms

| | |
|---|---|
| Performance of the service and deliverables: | <p>This Call-Off Contract will include delivery of the following milestones:</p> <p>Service performance and deliverables will be agreed and reviewed at monthly AMS review meetings against the SLAs stated above.</p> |
| Guarantee: | N/A |
| Warranties, representations: | N/A |
| Supplemental requirements in addition to the Call-Off terms: | Within the scope of the Call-Off Contract, the Supplier will not be required to make the IPR of any Project IPRs or Third Party IPR open source. |
| Alternative clauses: | N/A |
| Buyer specific amendments to/refinements of the Call-Off Contract terms: | <p>In accordance with Call-Off Contract clauses, the Supplier will adhere to the Buyers Special Terms as set out in Annex A</p> <p>The Buyer Special Terms shall form part of this Call-Off Contract. In the event of conflict, the order of precedence shall be as follows:</p> <ul style="list-style-type: none"> • G-Cloud 11 Framework Agreement |

| | |
|---|---|
| | <ul style="list-style-type: none"> • G-Cloud 11 Order Form • G-Cloud 11 Call-Off Contract • Buyer Supplemental Security clauses • Supplier Terms and Conditions |
| Public Services Network (PSN): | N/A |
| Personal Data and Data Subjects: | Yes - Annex 1 Schedule 7 is being used |

1. Formation of contract

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

2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.
- (B) The Buyer provided an Order Form for Services to the Supplier.

| | | |
|-------------------|------------|------------|
| Signed: | Supplier | Buyer |
| Name: | <REDACTED> | <REDACTED> |
| Title: | | |
| Signature: | <REDACTED> | <REDACTED> |
| Date: | | |

Schedule 1 - Services

The Supplier shall provide Lot 3 Cloud Support in accordance with the service definition “Workday Implementation Services” – Service ID 357314460582574 of the Digital Market Place refers. This Service ID covers the following provisions:

Part E – Post-Deployment Support Services

| Services | |
|--|--|
| Supported Items | <p>The Supplier will support the following items for all Modules deployed by the Supplier during the Service Period:</p> <ul style="list-style-type: none">• Workday Configurations• Workday Business process and security• Workday Integrations• Workday Custom Reports <p>Collectively the Application Management Services (AMS).</p> |
| Additional Services | <p>The Customer may procure the following additional Services under this Order Form, at any time during the Service Period (or agreed extensions to it):</p> <p>1. Ad-Hoc professional services (Project Work) – using the Change Request Form.</p> |
| Service Period | 18/12/20 – 20/06/21 |
| AMS Service Hours | <p>UK: Monday to Friday 0900-1700 GMT Excluding UK public holidays* www.publicholidays.co.uk</p> <p>*Bank holidays are not classified as public holidays</p> |
| AMS incident logging procedure & Service desk number | <p>Incidents should be logged by the Buyer through the Supplier incident management application. In addition to raising an incident on the application, although not required, the Buyer may also contact the Kainos Service Desk</p> |

| Application Management Services (AMS) Service Description | |
|---|--|
| The AMS provided by the Supplier comprises: | |
| Service Management | <p>An available named Service Manager to:</p> <ul style="list-style-type: none">- assess and manage AMS;- respond to requests for service within the SLA and progress appropriately;- consultancy; |

| | |
|---------------------------------|--|
| | <ul style="list-style-type: none"> - set up and on-going access to the Supplier incident management application for the Buyer including Incident history and traceability until completed investigation; - monthly MI reporting; - quarterly service reviews. |
| Telephone Advice and Assistance | To address Buyer enquiries in respect of the use or operation of the Supported Items during the Service Hours, within the Service Period. |
| Reporting Services | <ul style="list-style-type: none"> - the provision of status updates by Supplier to the Buyer in the form of monthly status reports detailing Incidents raised; - SLA metrics; - any potential recommendations or AMS improvements; - quarterly status meetings with the Buyer to review the AMS. |
| 3rd and 4th Tier Support | <ul style="list-style-type: none"> - provision of temporary or permanent corrections to the Supported Items where Incidents have been escalated from 1st and 2nd Line Tier (and where approval has been provided) to implement changes that cover: <ul style="list-style-type: none"> o test of correction or changes on the client non-Production environment; and o deployment of correction or change to the Production environment; - qualified personnel to provide support during the Service Hours and investigate Incidents with the Supported Items; - provision of consultancy services to Buyer's 1st and 2nd Tier Support (if required); - provision of estimates on the length of time to correct Incidents; - investigation and assessment of any Third Party Software changes and the possible impact on the Workday Service with recommended actions; - augment Buyer support teams with Supplier AMS staff (if required); - deliver configuration review and optimisation programmes (if required). |

The Buyer will:

- provide 1st and 2nd Tier Support, this involves:
 - performing initial investigation and assessment of Incidents (to include liaising with Buyer users to obtain all the relevant detail and error analysis information);
 - resolving straightforward issues and Incidents (for example and without limitation, data issues or simple configuration changes);
 - logging Incidents requiring more detailed investigation and providing a full description and information in the Kainos incident management application);
 - prioritising Incidents based on the Incident classifications set out in the Order Form;
 - providing interface between 3rd and 4th Tier Support and Buyer users and providing Incident feedback and appropriate workarounds to Buyer users;
 - keeping informed of Workday Updates and supply details to Buyer users on new features;
 - facilitating testing of changes on non-Production environment;
 - scheduling changes that need to be applied by Supplier to the production system (once testing has been confirmed as successful);
 - managing Third Party Software supplier relationships and the notification of changes to Supplier (via the Kainos incident management application) of any Third Party Software systems to allow Supplier to impact assess the changes on the Workday Service;
 - close Incidents;
- support any software or equipment with which the Supported Items or Workday Service interacts;
- liaise directly with Workday for resolution of Workday Service issues;
- ensure Workday Update regression test activities are planned and executed in timely manner;
- fulfil its obligations under the Order Form.

Further details on the service provision is available within the Service Definition document from G-Cloud. Link below:



Service Definition

Schedule 2 - Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed estimated Charges breakdown for the provision of Services during the Term will include:

<REDACTED>

The value above represents the full potential value of this contract. It does however contain optional costs for additional support days.

The contract value for the initial 5-month term is up to £78,000 (excluding VAT).

Further details on the SFIA rate card from the Service Offering on Cloud.



Costs

Part B - Terms and conditions

1. Call-Off Contract start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)

- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

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

3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

- 4.1 The Supplier Staff must:
- be appropriately experienced, qualified and trained to supply the Services
 - apply all due skill, care and diligence in faithfully performing those duties
 - obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
 - respond to any enquiries about the Services as soon as reasonably possible
 - complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and

promptly provide a copy to the Buyer.

- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

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

6. Business continuity and disaster recovery

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

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay

undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for

accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

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

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

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

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the

legal validity of the insurance.

- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
- premiums, which it will pay promptly
 - excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

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

11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above

and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

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

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

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

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

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

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

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

13. Buyer data

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

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

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

as requested.

- 13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.
- 13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
- the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
 - guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
 - the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/collection/risk-management-collection>
 - government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
 - the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
- 13.6 The Buyer will specify any security requirements for this project in the Order Form.

- 13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

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

- 16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

- 17.1 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:
- an executed Guarantee in the form at Schedule 5
 - 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:

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

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

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

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

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

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data); 19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

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

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

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

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

20. Notices

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

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

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

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

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

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

22. Handover to replacement supplier

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

23. Force majeure

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

24. Liability

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

technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

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

25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
- comply with any security requirements at the premises and not do anything to weaken the security of the premises
 - comply with Buyer requirements for the conduct of personnel
 - comply with any health and safety measures implemented by the Buyer

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

28.2 The Supplier must provide reasonable support to enable Buyers to work in an

environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

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

- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

Supplier may agree.

30. Additional G-Cloud services

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

31. Collaboration

- 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:
- work proactively and in good faith with each of the Buyer's contractors
 - co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

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

- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.
- 32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

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

Schedule 3 – Not Used

Schedule 4 – Alternative clauses – Not Used

Schedule 5 – Guarantee – Not Used

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

| | |
|---|---|
| Audit | An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any). |
| Background IPRs | <p>For each Party, IPRs:</p> <p>owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract, or</p> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p> |
| Buyer | The contracting authority ordering services as set out in the Order Form. |
| Buyer Data | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer. |
| Buyer Personal Data | The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract. |
| Buyer Representative | The representative appointed by the Buyer under this Call-Off Contract. |
| Buyer Software | Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services. |
| Call-Off Contract | This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement. |
| Charges | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract. |
| Collaboration Agreement | An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate. |
| Commercially Sensitive Information | Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive. |
| Confidential Information | Data, personal data and any information, which may include (but isn't limited to) any: |

| | |
|--|---|
| | information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential'). |
| Control | 'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly. |
| Controller | Takes the meaning given in the GDPR. |
| Crown | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf. |
| Data Loss Event | event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach |
| Data Protection Impact Assessment | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| Data Protection Legislation (DPL) | Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner . |
| Data Subject | Takes the meaning given in the GDPR |
| Default | Default is any: breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is |

| | |
|--|---|
| | liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer. |
| Deliverable(s) | The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract. |
| Digital Marketplace | The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/) |
| DPA 2018 | Data Protection Act 2018. |
| Employment Regulations | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive. |
| End | Means to terminate; and Ended and Ending are construed accordingly. |
| Environmental Information Regulations or EIR | The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations. |
| Equipment | The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract. |
| ESI Reference Number | The 14 digit ESI reference number from the summary of outcome screen of the ESI tool. |
| Employment Status Indicator test tool or ESI tool | The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi |
| Expiry Date | The expiry date of this Call-Off Contract in the Order Form. |
| Force Majeure | <p>A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <p>acts, events or omissions beyond the reasonable control of the affected Party</p> <p>riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</p> <p>acts of government, local government or Regulatory Bodies</p> <p>fire, flood or disaster and any failure or shortage of power or fuel</p> <p>industrial dispute affecting a third party for which a substitute third party isn't reasonably available</p> <p>The following do not constitute a Force Majeure event:</p> |

| | |
|---|--|
| | <p>any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</p> <p>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</p> <p>the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</p> <p>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</p> |
| Former Supplier | A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor). |
| Framework Agreement | The clauses of framework agreement RM1557.11 together with the Framework Schedules. |
| Fraud | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown. |
| Freedom of Information Act or FoIA | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation. |
| G-Cloud Services | The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement. |
| GDPR | The General Data Protection Regulation (Regulation (EU) 2016/679). |
| Good Industry Practice | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |
| Government Procurement Card | <p>The Government's preferred method of purchasing and payment for low value goods or services</p> <p>https://www.gov.uk/government/publications/government-procurement-card--2.</p> |

| | |
|---|---|
| Guarantee | The guarantee described in Schedule 5. |
| Guidance | Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence. |
| Implementation Plan | The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding. |
| Indicative Test | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6. |
| Information | Has the meaning given under section 84 of the Freedom of Information Act 2000. |
| Information Security Management System | The information security management system and process developed by the Supplier in accordance with clause 16.1. |
| Inside IR35 | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool. |
| Insolvency Event | Can be: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium. |
| Intellectual Property Rights or IPR | Intellectual Property Rights are: copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction all other rights having equivalent or similar effect in any country or jurisdiction |
| Intermediary | For the purposes of the IR35 rules an intermediary can be: the supplier's own limited company a service or a personal service company a partnership |

| | |
|-------------------------------|--|
| | It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). |
| IPR Claim | As set out in clause 11.5. |
| IR35 | IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary. |
| IR35 Assessment | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35. |
| Know-How | All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date. |
| Law | Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body. |
| LED | Law Enforcement Directive (EU) 2016/680. |
| Loss | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly. |
| Lot | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly. |
| Malicious Software | Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence. |
| Management Charge | The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract. |
| Management Information | The management information specified in Framework Agreement section 6 (What you report to CCS). |

| | |
|---------------------------------|---|
| Material Breach | Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract. |
| Ministry of Justice Code | The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000. |
| New Fair Deal | The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended. |
| Order | An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes. |
| Order Form | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services. |
| Ordered G-Cloud Services | G-Cloud Services which are the subject of an Order by the Buyer. |
| Outside IR35 | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool. |
| Party | The Buyer or the Supplier and 'Parties' will be interpreted accordingly. |
| Personal Data | Takes the meaning given in the GDPR. |
| Personal Data Breach | Takes the meaning given in the GDPR. |
| Processing | Takes the meaning given in the GDPR |
| Processor | Takes the meaning given in the GDPR. |
| Prohibited Act | <p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <p>induce that person to perform improperly a relevant function or activity</p> <p>reward that person for improper performance of a relevant function or activity</p> <p>commit any offence:</p> <p>under the Bribery Act 2010</p> <p>under legislation creating offences concerning Fraud</p> <p>at common Law concerning Fraud</p> <p>committing or attempting or conspiring to commit Fraud</p> |
| Project Specific IPRs | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but |

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

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

Schedule 7 - GDPR Information

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

Annex 1 - Processing Personal Data

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

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

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | The Buyer is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor. |
| Duration of the Processing | The term of this Call-Off Contract. |
| Nature and purposes of the Processing | The processing is needed, and restricted to, the Workday HR, Payroll and Expenses functionality within the Buyer's Organisation to ensure that the Supplier can effectively deliver the contract to successfully implement the Buyer's Workday functionality. This will involve data migration; data validation / testing; and Workday Application Management Services to provide Workday HR, Payroll, Data and Integrations support. |

| | |
|-----------------------------------|--|
| <p>Type of Personal Data</p> | <p>The type of Personal data includes:</p> <ul style="list-style-type: none"> • name, • address, • date of birth, • NI number, • telephone number, • pay, • contact information (including home and work address, phone numbers, next of kin details), • marital status, • ethnicity, • bank details, • gender, disability information, • employee identification number, • probation period, • visa information; • passport information; • military service information; • religion information; • education, • language(s) and special competencies; • certification information; • probation period and employment duration information; • job or position title; • cost center work schedule/pattern (full-time or part-time, regular or temporary); • compensation and related information (including pay type and information regarding raises and salary adjustments); • payroll information; • allowance, bonus, commission; • leave of absence information; • employment history; • training and development information; • award information; and • membership information. |
| <p>Categories of Data Subject</p> | <p>The Personal Data processed concern the following categories of data subjects:</p> <ul style="list-style-type: none"> • Controller staff, candidates, former staff (including full time, part time, contract/temporary staff and affiliates) |

| | |
|--|--|
| | <ul style="list-style-type: none"> Dependents / beneficiaries of Controller staff where benefits records are in scope |
| <p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p> | <p>At the written direction of the Buyer, the Supplier will delete or return Personal Data (and any copies of it) to the Buyer on termination of the Agreement, unless the Supplier is required by Law to retain the Personal Data in accordance with the relevant provisions of Terms and Conditions.</p> |

Annex 2 - Joint Controller Agreement – Not Used

Library of Clauses: Departmental Security Standards

(NB numbering relates to DFE internal documents)

12. Departmental Security Standards for Business Services and ICT Contracts

| | |
|--|---|
| <p>“BPSS” “Baseline Personnel Security Standard”</p> | <p>a level of security clearance described as pre-employment checks in the National Vetting Policy. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</p> |
| <p>“CCSC” “Certified Cyber Security Consultancy”</p> | <p>is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy</p> |
| <p>“CCP” “Certified Professional”</p> | <p>is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-professional</p> |
| <p>“CC” “Common Criteria”</p> | <p>the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.</p> |
| <p>“CPA” “Commercial Product Assurance” [formerly called “CESG Product Assurance”]</p> | <p>is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa</p> |
| <p>“Cyber Essentials” “Cyber Essentials Plus”</p> | <p>Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: https://www.iasme.co.uk/apply-for-self-assessment/</p> |

| | |
|--|--|
| <p>"Data"</p> <p>"Data Controller"</p> <p>"Data Processor"</p> <p>"Personal Data"</p> <p>"Sensitive Personal Data"</p> <p>"Data Subject", "Process" and "Processing"</p> | <p>shall have the meanings given to those terms by the Data Protection Act 2018</p> |
| <p>"Department's Data"</p> <p>"Department's Information"</p> | <p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including:</p> <p>(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:</p> <p>(i) supplied to the Contractor by or on behalf of the Department; or</p> <p>(ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or</p> <p>(b) any Personal Data for which the Department is the Data Controller;</p> |
| <p>"DfE"</p> <p>"Department"</p> | <p>means the Department for Education</p> |
| <p>"Departmental Security Standards"</p> | <p>means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.</p> |
| <p>"Digital Marketplace / GCloud"</p> | <p>the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.</p> |
| <p>"FIPS 140-2"</p> | <p>this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled 'Security Requirements for Cryptographic Modules'. This document is the de facto security standard used for the accreditation of cryptographic modules.</p> |
| <p>"Good Industry Practice"</p> <p>"Industry Good Practice"</p> | <p>means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.</p> |
| <p>"Good Industry Standard"</p> <p>"Industry Good Standard"</p> | <p>means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.</p> |

| | |
|--|---|
| <p>“GSC”</p> <p>“GSCP”</p> | <p>means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications</p> |
| <p>“HMG”</p> | <p>means Her Majesty’s Government</p> |
| <p>“ICT”</p> | <p>means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution</p> |
| <p>“ISO/IEC 27001” “ISO 27001”</p> | <p>is the International Standard for Information Security Management Systems Requirements</p> |
| <p>“ISO/IEC 27002” “ISO 27002”</p> | <p>is the International Standard describing the Code of Practice for Information Security Controls.</p> |
| <p>“ISO 22301”</p> | <p>is the International Standard describing for Business Continuity</p> |
| <p>“IT Security Health Check (ITSHC)”</p> <p>“IT Health Check (ITHC)”</p> <p>“Penetration Testing”</p> | <p>means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.</p> |
| <p>“Need-to-Know”</p> | <p>the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.</p> |
| <p>“NCSC”</p> | <p>The National Cyber Security Centre (NCSC) formerly CESG is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk</p> |
| <p>“OFFICIAL”</p> <p>“OFFICIAL-SENSITIVE”</p> | <p>the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services.</p> <p>the ‘OFFICIAL–SENSITIVE’ caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.</p> |
| <p>“Secure Sanitisation”</p> | <p>Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable. Secure sanitisation was previously covered by “Information Assurance Standard No. 5 - Secure Sanitisation” (“IS5”) issued by the former CESG. Guidance can now be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</p> |

| | |
|---|--|
| | <p>The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction</p> |
| <p>“Security and Information Risk Advisor” “CCP SIRA” “SIRA”</p> | <p>the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</p> |
| <p>“SPF” “HMG Security Policy Framework”</p> | <p>This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework</p> |
| <p>“Tailored Assurance” [formerly called “CTAS”, or, “CESG Tailored Assurance”]</p> | <p>is an ‘information assurance scheme’ which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology</p> |

- 1.1. The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
- 1.2. Where the Contractor will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - [Action Note 09/14](#) 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme”. The certification scope must be relevant to the services supplied to, or on behalf of, the Department.
- 1.3 The Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
- 1.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
- 1.5 Departmental Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Contractor and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.

- 1.6 The Contractor shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas.
- 1.7 The Contractor shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.
- 1.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.
- 1.9 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which has been certified to FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.
- 1.10 Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.11 and 1.12 below.
- 1.11 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.
- 1.12 All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.
- 1.13 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.
- 1.14 When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.
- 1.15 At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Contractor's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.
- 1.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone

mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff who have access to Departmental Data must complete this process before access to Departmental Data is permitted.

- 1.17 All Contractor or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.
- 1.18 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 1.19 Any breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, or any non-compliance with these Departmental Security Standards for Contractors, or other agreed Security Standards pertaining to the solution, shall be investigated immediately and escalated without undue delay to the Department by a method agreed by both parties.

- 1.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required. The Contractor or sub-contractors providing the service will provide the Department with full details of any storage of Departmental Data outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Contractor or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department. The Department reserves the right to audit the Contractor not more than once per annum providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors, compliance with the clauses contained in this Section. The Contractor will co-operate and provide assistance at Department cost (such co-operation including the provision of any reports provided to the Contractor by sub-contractors where available and where the Contractor is permitted to disclose those to the Department).
- 1.21 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who have access to Departmental Data in the course of providing this service.
- 1.22 The Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA).
- 1.23 Where the Contractor is delivering an ICT solution to the Department they shall deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:
- Any existing security assurance for the services to be delivered such as the Common Criteria (CC) and ISO 27001 or an equivalent industry level certification.
 - Existing HMG security accreditations or assurance that are still valid including: details of the body awarding the accreditation; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement. Documented evidence of any existing security accreditation shall be required.
 - Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

General Clauses

Contractor's Standards

The Contractor shall as far as practicable satisfy the Department that it operates to, or is working towards, an acceptable standard such as BS 5750, BS EN ISO 9000, ISO 9001 or an equivalent.

Supplier T's and C's



Kainos T's and C's