



Crown
Commercial
Service

G-Cloud 13 Call-Off Contract

Between

**The Secretary of State for
The Department for Education**

And

NTT DATA UK Limited

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

G-Cloud 13 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	15
Schedule 1: Services	36
Schedule 2: Call-Off Contract charges	37
Schedule 3: Collaboration agreement	38
Schedule 4: Alternative clauses	51
Schedule 5: Guarantee	56
Schedule 6: Glossary and interpretations	65
Schedule 7: UK GDPR Information	83
Annex 1: Processing Personal Data	84
Annex 2: Joint Controller Agreement	89

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	689083206893298
Call-Off Contract reference	project_8159 Con_20912
Call-Off Contract title	IRIS365 – BAU support for Microsoft Dynamics 365 platform
Call-Off Contract description	Support and maintenance of the IRIS365 system
Start date	01/08/2023
Expiry date	31/07/2026 (with provision for a further 12-month extension, subject to internal approvals)
Call-Off Contract value	<p>Potential total Call-Off Contract value is up to a maximum of £864,920 (excluding VAT) £1,037,904.00 (including VAT).</p> <p>This consists of 2 elements:</p> <ol style="list-style-type: none">1) a fixed price of £116,230 annually (excluding VAT) for the Core Services as defined in Schedule 1, billed monthly as a support fee of £9685.83 (excluding VAT) for 12 months. (£348,690 for the 3 year contract, plus a potential additional £116,230 for the extension provision).2) a non-committed additional £400,000 (excluding VAT) available for the Additional Services defined in Schedule 1, which include minor enhancements/break fix. <p>£400,000 is the maximum additional spend allowed and each piece of work would be contracted under a separate Statement of Work issued pursuant to a Request for Quotation with additional Department for Education (DfE) approval required prior</p>

	to work commencing/spend being made against this provision.
Charging method	<p>The Supplier shall issue electronic invoices monthly based on payment profiles at Schedule 2.</p> <p>The Supplier shall issue electronic invoices via BACS based on payment profiles at Schedule 2.</p>
Purchase order number	<p>To be confirmed and issued after contract signature.</p> <p>PO and contract reference number to be quoted on all invoicing.</p> <p>No work must be undertaken until supplier is in receipt of an official Purchase Order</p>

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

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

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

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

From the Buyer	The Secretary of State for the Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
To the Supplier	<p>NTT DATA UK Ltd 2 Royal Exchange London EC3V 3DG</p> <p>Company number: 03085018</p>
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Senior Contract Manager

Name: [REDACTED]

Email: [REDACTED]

For the Supplier:

Title: Vice President and Client Partner

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01/08/2023 and is valid until 31/07/2026 (36 months) with provision for a further 12-month extension, subject to internal approvals.
Ending (termination)	<p>The contract shall expire 31st July 2026 unless terminated sooner. The notice period for the Supplier needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p> <p>The notice period for the Buyer to terminate an individual SOW is a maximum of 5 Working Days from the date of written notice for termination without cause.</p> <p>Regarding Charges per each Statement of Works (SOW), the Parties, acting reasonably, will agree any charges due for Contracted Out Services on a proportional basis reflecting a reasonable compensation for the price of work already completed if the date of termination is prior to the next milestone payment date.</p> <p>For Resource Driven Services based charges, the Buyer will pay the Supplier the charges based on days utilised up to the date of termination.</p>

Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier four weeks written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Buyer contractual details

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

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 3 Cloud Support
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <ul style="list-style-type: none"> • G-Cloud 13 Service Offering • Service ID 689083206893298 <p>The Buyer has requested the Supplier provide specific Services in accordance with the terms set out in this Call-Off Contract.</p> <p>These services are detailed in Schedule 1 to this Order Form and summarised below.</p> <p>The Core Services include support and maintenance of the CRM Dynamics 365 environment (IRIS365) which resides on DfE's Microsoft Azure instance, working to agreed SLAs and KPI availability information.</p> <p>The Supplier will be expected to work alongside DfE internal IT teams who support other elements of the application such as the hosting provider and other teams such as the Exchange admin team and DfE's Knowledge Management team (integrated SharePoint online support).</p> <p>DfE shall be able to raise a Request for Quotation (RFQ) with the Supplier to request Additional Services such as ad-hoc software and functional development work, which shall be authorised and contracted via a separate Statement of Work (SOW). There may be a requirement in the future to expand the current IRIS build to include other business functionality. DfE require the Supplier to</p>

	plan, support and deploy Microsoft's EverGreen approach to updates for CRM Dynamics 365.
Additional Services	DfE require the ability to raise and request RFQ's with the supplier for ad-hoc software and functional development work. There may be a requirement in the future to expand the current IRIS build to include other business functionality. DfE require a supplier to plan, support and deploy Microsoft's EverGreen approach to updates for CRM Dynamics 365.
Location	<p>The Primary Location of Work for the purpose of this Agreement shall be the Supplier's own premises.</p> <p>The Buyer does not prescribe the location the services will be delivered, however there is likely to be a requirement that the Supplier will attend key Buyer sites.</p> <p>The Services will be delivered remotely or at DfE offices below if necessary:</p> <p>Primarily these may include, but not be limited to:</p> <p><u>Manchester</u> Department for Education Piccadilly Gate, Store Street, Man- chester, M1 2W</p> <p><u>London</u> Sanctuary Buildings, Great Smith Street, London, SW1P 3B</p> <p>All data related to the Services will be stored on DfE Environments and equipment.</p> <p>For additional Services undertaken under a SOW, the locations will be agreed with the Supplier for each Statement of Work.</p> <p>The Buyer may require work to be delivered at any Buyer site within England. Expenses cannot be claimed for travel or subsistence at the Primary Location of Work. Expenses can be claimed for travel or subsistence to any other location of work. All Supplier expenses must be in line with the Buyer's prevailing expenses policy, which shall not be unreasonable and shall be provided to the Supplier upon request with revised versions issued from time-to-time if and when this is updated.</p>

Quality Standards	<p>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 Buyer's requirements and in line with G-Cloud 13 offerings and in accordance with ISO 9001: 2013. The supplier is expected to work in an 'Agile' way, to support customer (DDaT Group and DfE) and also to any clauses at Annex A. The quality standards required for this Call-Off Contract are:</p> <p><input type="checkbox"/> ISO9000, ISO 27001 and ISO 20000 accreditation</p> <p>Service Management Framework aligned with ITIL v3..</p> <p>Any specific quality standards required will be detailed in the individual Statement of Works.</p>
Technical Standards:	<p>Any specific technical standards required will be detailed in the individual work package.</p> <p>The technical standards used as a requirement for this Call-Off Contract are as set-out in the Supplier's published service definition under the Service reference stated at the Schedules of this Order Form.</p>
Service level agreement:	<p>The service level and availability criteria required for the Core Services are detailed in Schedule 1, to this Order Form.</p> <p>For Additional Services, any specific Service Level requirements will be stated in the RFQ and included in the individual SOW if required.</p> <p>On receipt of an RFQ, the Supplier is to provide their response within 6 working days (48 working hours) unless otherwise agreed between the Buyer and Supplier.</p> <p>Supplier to provide a service report using the agreed template in ANNEX C within 5 Working Days of the first Working Day of each calendar month, reporting on the previous month's activity and financials.</p> <p>Supplier will minute any items requiring action within the set Action Log within 3 Working Days of the Contract Review taking place.</p> <p>The service level and availability criteria required for this Call-Off Contract are:</p> <p>Incidents and requests are assigned a priority, depending on the impact and urgency of the issue. Technology Directorate and its</p>

suppliers must aim to respond and resolve issues against their incident priority level, set out in the table below:

Priority	Target Response	Target Update	Target Resolution
P1	15 minutes	Every hour	4 hours
P2	1 hour	Every 4 hours	1 day
P3	1 day	Every 2 days	5 days
P4	2 days	On request	5 days
P5	3 days	On request	15 days

The service should be available 24/7 within supported Operational Hours (defined as 09:00-17:00, Monday – Friday on Working Days only).

Overall service availability during Operational Hours is 99.9% and 99.5% at all other times.

The following table explains how the priority levels are assigned based on the incident and its impact to the business.

Priority	Description and examples
Priority 1 (P1) - Major Incident	<p>An Incident causing an extremely serious impact to the business, as a result of the system(s) / service(s) affected and/or the number of people affected by the Incident, e.g.</p> <ul style="list-style-type: none"> - The Incident affects more than 50% of all service users; and the service affected is a core business service / function; and areas outside of DfE are affected; or - A business unit is halted completely.
Priority 2 (P2) - Significant	<p>An Incident causing significant impact to the business as a result of the system(s) / service(s) affected and/or the number of people affected by the Incident, e.g.</p> <ul style="list-style-type: none"> - The Incident affects between 25% and 50% of all service users; and the service affected is a core business service / function; or - The Incident affects more than 50% of all service users; and the service affected is a non-core business service / function.

	<p>Priority 3 (P3) - Minimal</p> <p>An Incident causing minimal impact to the business as a result of the system(s)/service(s) affected and/or the number of people affected by the Incident, e.g.</p> <ul style="list-style-type: none"> - The Incident affects less than 25% of all service users; and the service affected is a core business service/function; or - The Incident affects less than 50% of all service users; and the service affected is a non-core business service / function; or - A single user is unable to perform their core daily business function effectively.
	<p>Priority 4 (P4) - Negligible</p> <p>An Incident causing negligible impact to the business as a result of the system(s)/service(s) affected and/or the number of people affected by the Incident, e.g.</p> <ul style="list-style-type: none"> - The Incident affects a single user, regardless of service type; or - The service affected is not managed by Technology Directorate
	<p>Priority 5 (P5) - Service Request</p> <p>A Service Request that may require submission to the Technology Directorate Change Advisory Board (CAB) or that requires procurement of equipment, e.g.</p> <ul style="list-style-type: none"> - A request for a new device; or - A new version of software that needs CAB approval and testing.
Onboarding	<p>The Supplier shall ensure that any personnel on boarded shall meet the requirements of the Buyer's Baseline Personnel Security Standard Policy unless otherwise stated within an RfQ HMG personnel security controls - GOV.UK (www.gov.uk).</p> <p>If applicable, the Buyer's assumption is on-boarding will begin with a Supplier kick-off meeting at a Supplier site with all key stakeholders. The areas for on-boarding discussion to include:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Roles and responsibilities within respective organisations (DfE & NTT); <input type="checkbox"/> Support model including use of Service Now and triage model; <input type="checkbox"/> Access requirements for Day 1 (where applicable);

	<ul style="list-style-type: none"> <input type="checkbox"/> Supplier/Service Management model/wrap (regular KIT's, service reviews, etc.); <input type="checkbox"/> Commercial/Contract Management expectations and financials; <input type="checkbox"/> Business context (requirements, business criticality, performance needs/peak times); <input type="checkbox"/> Potential CSIP's; <input type="checkbox"/> Timetable of activities; <input type="checkbox"/> Licensing. <p>Follow up sessions may be required as part of outcomes with specific technical teams to ensure processes and access are in place for the start of the contract.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>In accordance with the provisions of clause 21, the Supplier shall produce an initial Exit plan.</p> <p>The off-boarding plan for this Call-Off Contract shall be agreed between the parties within 6 weeks of the start of contract 'go live' date and re-reviewed three (3) months from the expiry date of the Call-Off Contract, in the form of an agreed exit plan.</p> <ul style="list-style-type: none"> • This will involve details of the process for ensuring the transfer of knowledge to the Buyer, a representative nominated by the Buyer or a different Supplier. • The offboarding plan will be reviewed 1 week prior to the end of the Services. The Buyer and Supplier will confirm and agree the offboarding activity. If appropriate, the supplier will submit costings for professional services to be used in the process for approval by the Buyer. <p>Supplier staff will return DfE equipment on the day that the contractor finishes their duties following guidance provided by DfE.</p>
Offboarding	
Collaboration agreement	Not applicable

Limit on Parties' liability	<p>Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £1 million.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed 125% of the Charges for the specific Statement of Works to which the default relates in default payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability of the Supplier for all other Defaults will Not exceed 125% of the Charges payable by the Buyer to the Supplier during the preceding 12 months of the Call-Off Contract Term.</p>
Insurance	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> • a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 10 consecutive days.</p> <p>This section relates to clause 23.1 in Part B below.</p>

Audit

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.

List of the required audit provisions from clauses 7.3 to 7.13 of the Framework Agreement:

What will happen during the Framework Agreement's Term

7.3 The Supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the:

- operation of the Framework Agreement and the Call-Off Contracts entered into with Buyers
- Services provided under any Call-Off Contracts (including any Subcontracts)
- amounts paid by each Buyer under the Call-Off Contracts

What will happen when the Framework Agreement ends

7.4 The Supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the:

7.4.1 operation of the Framework Agreement and the Call-Off Contracts entered into with Buyers

7.4.2 Services provided under any Call-Off Contracts (including any Subcontracts)

7.4.3 amounts paid by each Buyer under the Call-Off Contracts

What will happen when the Framework Agreement Ends

7.5 The Supplier will provide a completed self audit certificate (Schedule 2) to CCS within 3 months of the expiry or Ending of this Framework Agreement.

7.6 The Supplier's records and accounts will be kept until the latest of the following dates:

7.6.1 7 years after the date of Ending or expiry of this Framework Agreement

7.6.2 7 years after the date of Ending or expiry of the last Call-Off Contract to expire or End

7.6.3 another date agreed between the Parties

7.7 During the timeframes highlighted in clause 7.6, the Supplier will maintain:

7.7.1 commercial records of the Charges and costs (including Subcontractors' costs) and any variations to them, including proposed variations

7.7.2 books of accounts for this Framework Agreement and all Call-Off Contracts

7.7.3 MI Reports

7.7.4 access to its published accounts and trading entity information

7.7.5 proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Framework Agreement

7.7.6 records of its delivery performance under each Call-Off Contract, including that of its Subcontractors

What will happen during an audit or inspection

7.8 CCS will use reasonable endeavours to ensure that the Audit does not unreasonably disrupt the Supplier, but the Supplier accepts that control over the conduct of Audits carried out by the auditors is outside of CCS's control.

7.9 Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to:

7.9.1 provide audit information without delay

7.9.2 provide all audit information within scope and give auditors access to Supplier Staff

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

7.10.1 the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement)

7.10.2 any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and

Management Charges under the Framework Agreement and Call-Off Contract only

7.10.3 the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier

7.10.4 any other aspect of the delivery of the Services including to review compliance with any legislation

7.10.5 the accuracy and completeness of any MI delivered or required by the Framework Agreement

7.10.6 any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records

7.10.7 the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date Costs of conducting audits or inspections

7.11 The Supplier will reimburse CCS its reasonable Audit costs if it reveals:

7.11.1 an underpayment by the Supplier to CCS in excess of 5% of the total Management Charge due in any monthly reporting and accounting period

7.11.2 a Material Breach

7.12 CCS can End this Framework Agreement under Section 5 (Ending and suspension of a Supplier's appointment) for Material Breach if either event in clause 7.11 applies.

7.13 Each Party is responsible for covering all their own other costs incurred from their compliance with the Audit obligations.

<p>Buyer's responsibilities</p>	<p>The Buyer is responsible for the provision of access to the Buyer's premises where services are to be delivered together with adequate desk space and office facilities including access to the Buyer's IT systems, staff and subcontractors, together with specific responsibilities as detailed in Schedule 1.</p> <p>The Buyer will also ensure:</p> <ul style="list-style-type: none"> • Access to appropriately experienced Points of Contact necessary for the delivery of the Services and to receive knowledge transfer from NTT. • Those decisions necessary to progress the Services are not unreasonably delayed or withheld. • making available its own representatives and its 3rd party suppliers for meetings and promptly provide information, materials and documents reasonably requested by the Supplier from time to time; • to provide the proposed reporting timetable and report formats for governance and meetings and; • be responsible for communication to its organisation in respect of any agreed activity by the Supplier when understating services defined within this Call Off Contract which may impact the Buyer's business
<p>Buyer's equipment</p> <p>Return of Buyer's equipment</p>	<p>As part of the on-boarding plan the Buyer will discuss with the Supplier the requirements and provide DfE equipment as appropriate.</p> <p>Any DfE equipment that is issued will be recorded and Annex A DfE Special Clauses will apply.</p> <p>All DfE provided remains the property of DfE.</p> <p>The Buyer's equipment to be used with this Call-Off Contract includes IT equipment to allow access to the Buyer's systems. The Buyer's equipment will be used where the Buyer's security and technical requirements necessitate.</p> <p>The Supplier will be required to provide an itinerary of all Buyer-provided IT equipment when requested.</p> <p>At the Ending or expiry of this Call-Off Contract (however arising), the Supplier must immediately deliver to the Buyer all equipment issued or made available to the Supplier in connection with this Call-Off Contract (the 'Buyer Equipment') in the Supplier's possession or under its control or in the possession or under the control of any Supplier Staff or any Subcontractor.</p> <p>If the Supplier does not deliver the Buyer Equipment to the Buyer as set out in clause 3.17, the Buyer may in its sole discretion:</p>

	<ul style="list-style-type: none"> (a) recover possession of such Buyer Equipment and the Supplier grants a licence to the Buyer and its agents to enter upon the premises of the Supplier to recover any such Buyer Equipment; (b) deduct a sum equivalent to the reasonable cost of replacing such Buyer Equipment from any amount due to the Supplier under this Call-Off Contract or under any other agreement between the Supplier and the Buyer; and/or (c) take any other action available under the terms of this Call-Off Contract or otherwise including commencing formal action. <p>The Supplier must ensure all Buyer Equipment is returned to the Buyer in good working order (allowance will be made only for reasonable wear and tear).</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Supplier's information

Subcontractors or partners	<p>The Supplier is not using any key third party subcontractor or partners in the delivery of services at the commencement of this call-off contract.</p> <p>However, where the Supplier uses third party subcontractor or partners in the delivery of services in the future, then these will be added to this call-off by means of a Variation.</p>
-----------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Call-Off Contract charges and payment

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

Payment method	<p>The payment method for this Call-Off Contract is by BACS transfer.</p> <p>The payment method for this Call-Off Contract is 30 days of the date on the invoice, by BACS for services/outputs delivered as detailed in the RFQ for each work package in accordance with Annex B RFQ Template</p>
Payment profile	<p>The payment profile for this Call-Off Contract is monthly in arrears as detailed at schedule 2</p>



Invoice details	<p>The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.</p> <p>All invoices should be issued to the principal contact for verification and approval prior to electronic submission process.</p> <p>All queries regarding payments or the settlement of invoices will be directed to the Buyer named in the RfQ/Purchase Order.</p> <p>General invoice and payment enquiries must not be directed to the Contract Manager.</p> <p>Where an invoice is submitted and paid prior to Acceptance Criteria being met, they will continue providing the services until Acceptance Criteria are fully satisfied at no additional cost to DfE.</p>
Who and where to send invoices to	<p>Invoices will be sent to:</p> <p>Department for Education</p> <p>DfE General</p> <p>Cheylesmore House</p> <p>Quinton Road</p> <p>Coventry</p> <p>CV1 2WT</p> <p>AccountsPayable.OCR@education.gov.uk</p>
Invoice information required	<p>The Invoice format will follow the standard Supplier invoice format inclusive of the G-Cloud Buyer Purchase Order.</p> <p>All invoices must include:</p> <ul style="list-style-type: none"> • The correct sum (in £ sterling) – in accordance with costs agreed with the Customer. • The correct terms of services/goods supplied • specification of the services supplied, confirming that agreed deliverables have been achieved within the applicable milestone period.

	<ul style="list-style-type: none"> • A unique invoice number • A valid purchase order number • Correct Supplier details, date, and contact details • Have been delivered to the nominated address • Have been delivered in timing in accordance with the contract <p>A copy invoice shall simultaneously be emailed to the DfE Buyer to enable the Buyer to take receipting action.</p>
Invoice frequency	<p>Invoices will be sent to the Buyer monthly.</p> <p>Invoice will be sent to the Buyer monthly in arrears according to the successful completion of work package outcomes and associated milestones, unless otherwise agreed through the Payment Schedule agreed in an RfQ.</p>
Call-Off Contract value	<p>The total value of this Call-Off Contract is £116,230 per year (potentially £464,920 for the full life of the 4-year term if the +1 option is taken) plus an optional uncommitted £400,000 minor enhancement capability. Total cost £864,920 (excl. VAT).</p>

Call-Off Contract charges	<p>The Call-Off Contract charges consists of two elements:</p> <p>1) a fixed price of £116,230 annually (excluding VAT) for the Core Services as defined in Schedule 1, billed monthly as a support fee of £9685.83 (excluding VAT) for 12 months. (£348,690 for the 3 year contract, plus a potential additional £116,230 for the extension provision).</p> <p>[REDACTED]</p> <p>2) a non-committed additional £400,000 (excluding VAT) available for the Additional Services defined in Schedule 1, which include minor enhancements/break fix.</p> <p>£400,000 is the maximum additional spend allowed and each piece of work would be contracted under a separate Statement of Work issued pursuant to a Request for Quotation with additional Department for Education (DfE) approval required prior to work commencing/spend being made against this provision.</p> <p>The additional spend may be utilised for SOWs either on a Fixed Price basis (for Contracted Out Services) or on a Time & Materials basis (for Resource Driven Services).</p> <p>The Charges for each SOW shall be agreed within each specific SOW . Resource Driven Services shall be priced against the agreed rates as follows:</p> <p>Supplier rate table:</p> <table border="1"> <thead> <tr> <th>SFIA Level</th><th>Day rate (GBP)</th></tr> </thead> <tbody> <tr><td>SFIA Level 1</td><td>[REDACTED]</td></tr> <tr><td>SFIA Level 2</td><td>[REDACTED]</td></tr> <tr><td>SFIA Level 3</td><td>[REDACTED]</td></tr> <tr><td>SFIA Level 4</td><td>[REDACTED]</td></tr> <tr><td>SFIA Level 5</td><td>[REDACTED]</td></tr> <tr><td>SFIA Level 6</td><td>[REDACTED]</td></tr> <tr><td>SFIA Level 7</td><td>[REDACTED]</td></tr> </tbody> </table>	SFIA Level	Day rate (GBP)	SFIA Level 1	[REDACTED]	SFIA Level 2	[REDACTED]	SFIA Level 3	[REDACTED]	SFIA Level 4	[REDACTED]	SFIA Level 5	[REDACTED]	SFIA Level 6	[REDACTED]	SFIA Level 7	[REDACTED]
SFIA Level	Day rate (GBP)																
SFIA Level 1	[REDACTED]																
SFIA Level 2	[REDACTED]																
SFIA Level 3	[REDACTED]																
SFIA Level 4	[REDACTED]																
SFIA Level 5	[REDACTED]																
SFIA Level 6	[REDACTED]																
SFIA Level 7	[REDACTED]																

Additional Buyer terms

Performance of the Service and Deliverables	<p>The Services shall be agreed and provided through Statement of Works that are identified as being made under this Call-Off Contract and which shall form part of this Order Form.</p> <p>This Call-Off Contract will include the following Deliverables and milestones, implementation plan, exit and off boarding plans outlined in Schedule 1 and the Statement of Work.</p>
----------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>All Supplier staff with access to DfE data or network will make themselves familiar and comply with the following:</p> <p>The HMG security policy framework describes the mandatory security outcomes expected of all of Her Majesty's Government's (HMG) organisations, and their partners handling HMG information.</p> <p>This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none"> <input type="checkbox"/> On-boarding activities to be agreed between DfE and supplier <input type="checkbox"/> Service Delivery is expected to commence on 1 August 2023. <input type="checkbox"/> Monthly Service & Contact Review meetings
Guarantee	Not Applicable
Warranties, representations	Not Applicable
Supplemental requirements in addition to the Call-Off terms	<p>Within the scope of the Call-Off Contract, the Supplier will:</p> <ol style="list-style-type: none"> 1. Comply with HMG Baseline Personnel Security Standard (BPSS)/ Government Staff Vetting Procedures Version 6.May 2018 attached below in respect of all persons who are employed or engaged by the Supplier in provision of Services under this Call-Off Contract, unless alternative agreement for personnel security is already in place between the Buyer and the Supplier. The HMG Baseline Personnel Security Standard / Government Staff Vetting Procedures Version 6.May 2018 do not require a security check as such but a package of pre-employment checks covering identity, employment history, nationality/immigration status and criminal records designed to provide a level of assurance. <div style="text-align: center;">  <p>HMG_Baseline_Personnel_Security_Standard</p> </div> <ol style="list-style-type: none"> 2. The Supplier agrees to the variations below to the Buyer standard clauses in respect of Information Security requirements, also attached at Annex A: <div style="text-align: center;">  <p>DfE additional clauses</p> </div>

Alternative clauses	Not Applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>The Buyer Supplemental Security clauses 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 13 Framework Agreement • G-Cloud 13 Order Form • G-Cloud 13 Call-Off Contract • Buyer Supplemental Security clauses and Conditions of Contract (Annex A) • Supplier Terms and Conditions <p>The expression “Contractor” within the Buyers Supplementary Security clauses and Conditions of Contract (Annex A) shall have the same meaning as “Supplier” as defined in Schedule 6 of this Order Form.</p>
Personal Data and Data Subjects	<p>Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: [Delete as appropriate] Annex 1, Annex 2</p> <p>Processing, Personal Data and Data Subjects: Under delivery of Specialist IT Commercial Services to DfE as described in this Call-Off contract, the Supplier shall not be processing any Personal Data and hence this Schedule 7 as referenced is not required.</p> <p>In the event that the Customer requires the Supplier to process data under the GDPR data processing provisions, this will be incorporated into the Call-Off Contract through following the Variation Procedure as detailed in the call off terms and the services.</p>
Intellectual Property	Not Applicable

Social Value	Not Applicable
---------------------	----------------

1. Formation of contract

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

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

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

Customer Benefits

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

[G-Cloud 13 Customer Benefit Record](#)

Part B: Terms and conditions

1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)

- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

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

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
- 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
 - 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
 - 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
 - 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of

£5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

9.8.1 premiums, which it will pay promptly

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

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

- 11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.
- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:
- 11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and
- 11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.
- 11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.
- 11.5 Subject to the limitation in Clause 24.3, the Buyer shall:
- 11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
 - (b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
 - (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and
- 11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:

<https://www.gov.uk/government/publications/government-securityclassifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.cpni.gov.uk/content/adopt-risk->

[managementapproach](https://www.cpni.gov.uk/protection-sensitive-information-and-assets) and Protection of Sensitive Information and Assets:
<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

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

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:
- 17.1.1 an executed Guarantee in the form at Schedule 5
- 17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.
- 18.2 The Parties agree that the:
- 18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- 18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses
- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)

- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

20. Notices

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

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

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

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

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

26. Equipment

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

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

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

28. Environmental requirements

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

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
 - 29.2.2 age
 - 29.2.3 start date
 - 29.2.4 place of work
 - 29.2.5 notice period
 - 29.2.6 redundancy payment entitlement
 - 29.2.7 salary, benefits and pension entitlements
 - 29.2.8 employment status
 - 29.2.9 identity of employer
 - 29.2.10 working arrangements
 - 29.2.11 outstanding liabilities
 - 29.2.12 sickness absence
 - 29.2.13 copies of all relevant employment contracts and related documents
 - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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.

29.3 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.

29.4 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.

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

29.5.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

Core Services

The Supplier shall provide the Core Services as per the service set out in Section 2.3 of the attached Service Definition document:



689083206893298-se
ervice-definition-docur

The service definition document is available within the G-Cloud 13 service offering within the Digital Marketplace. In the event of any conflict between the the Service Description and this Call-Off Contract, the requirements of this Call-Off Contract will prevail.

Additional Services

In addition to the Core Services, this Call-Off Contract can be used for the provision of Additional Services:

- (i) **Contracted Out Services** – These services have outcome based deliverables detailed in each individual SOW, based on Fixed Price charges. The award of these services is dependent upon sufficient definition of requirements in the RFQ to enable the Supplier to provide a Fixed Price quotation. The SOW shall define Deliverables and Acceptance Criteria, plus a Milestone Payment plan. These Acceptance Criteria will then be used by DfE to approve the successful completion of the relevant deliverable(s) (which is not to be unreasonably withheld prior to DfE authorising each Milestone Payment through a valid Milestone Acceptance Certificate. DfE's determination of acceptance must be provided within 5 Working Days of the Supplier's submission of the Deliverable. Where an invoice is submitted and paid prior to Acceptance Criteria being met, the Supplier will continue providing the services until Acceptance Criteria are fully satisfied at no additional cost to DfE.
- (ii) **Resource Driven Services** – These services are based on Time and Material charges for Supplier resources detailed in each individual SOW. Payment shall be conditional upon Time and Material costs incurred by the Supplier only, and shall not be conditional upon the achievement or acceptance of outcomes or deliverables, which shall be intended or expected outcomes only. The Buyer can use the Resource Driven Services to commission 'discovery' activities by the Supplier to inform its requirements definition for subsequent Contracted Out Services, if required.

1. A separate Change Authorisation Note (CAN) will be agreed by the Supplier and the Buyer for adding each individual SOW to this Call-Off Contract.
2. Prior to agreeing the CAN, the Buyer will conduct an assessment of the requirements to determine whether the SOW is for Resource Driven Services or Contracted Out Services and will request the Supplier to provide an associated proposal. The SOW will include details of how the services will be operated and will include the wording in 3.1(i) to (ii) or 3.2 (i to vi) below as appropriate:
 - 3.1. Where the SOW has been assessed as being for Resource Driven Services, the related SOW will be operated as follows:
 - (i) The Supplier warrants that it can deliver the related SOW using personnel who are on the Supplier's payroll and/or through subcontracts and/or umbrella company with full PAYE

and NI deducted for such personnel at source and therefore outside IR35 so as not to breach the terms of the G-Cloud Framework Agreement.

3.2. For any SOW added to this Call-Off Contract through the Variation process for a Resource Driven Services, the Supplier shall provide the information set out below to the Buyer and the Supplier shall comply with the obligations set out below, so that the Buyer can comply with its obligations with regards to the off-payroll working regime:

- a. Supplier Staff Name(s)
- b. Start and End date of the Engagement
- c. The contracted Day Rate of the Supplier Staff
- d. Is (Are) the Supplier Staff on a payroll and are deductions of PAYE and National Insurance made at source? Yes/No
- e. If "yes", then the provision of the fee payer details for each of the Supplier Staff (e.g, Supplier PAYE, Agent PAYE, Umbrella Company)
- f. Notification to the Buyer If the employment status of the Supplier Staff for tax purposes changes so that a fresh determination may be made as set out at 1.2 to 1.5 above
- g. The provisions at 1.2 to 1.7 above must be reviewed in the event of any proposed changes to this Order.

AND

Prior to the Supplier substituting any Supplier Staff, the Supplier shall;

- (ii) Confirm to the Buyer that it can continue to deliver the related SOW using personnel who are on the Supplier's payroll and/or through subcontracts and/or umbrella company with full PAYE and NI deducted for such personnel at source and therefore outside IR35 so as not to breach the terms of the G-cloud Framework.

3.2 Where the Statement of Works has been assessed as being a supply of Contracted Out Services, the related SOW will be operated as follows:

- (i) This SOW specifies outcome based deliverables detailed in a separate and clear table
- (ii) The Supplier Staff will be under the day to day direction and control of the Supplier, not DFE;
- (iii) Any quality and non-delivery issues will be raised by Erik Van-Kampen directly with the Supplier rather than the individual Supplier Staff;
- (iv) The Supplier will be held accountable by DFE for non-delivery of the services, not the individual Supplier Staff;
- (v) The Supplier is able to substitute the individual Supplier Staff to undertake the services within the related SOW as long as they have the equivalent experience and qualifications of the substituted individual Supplier Staff member;
- (vi) The related SOW will not be used to fill roles that already exist in DFE.

3. During the life of the Call-Off Contract, additional Services may be requested by the Buyer. These will be individually governed and attached to a separate CAN by following the Variation procedure (Clause 32) and subject to the Contract Value's specified at Section 5.7.

4. The Supplier shall commit to add the following additional value under this Contract:

- (i) Statement of Works specific discounts;
 - (a) When providing a quote for any Statement of Works under this Contract (whether for resource or contracted-out service), the Supplier shall consider all opportunities to

provide the best value for money for the Buyer, and shall report on any discounts applied;

(b) When providing a quote for any Statements of Works under this Contract, the Supplier shall consider at its own discretion whether the following discounts can be available to the Buyer (this list is not exhaustive);

- **Blended Team Model**

- The ability to utilise a blended team model for outcome based services on each specific Statement of Work (SOW)
- The ability to utilise a blended team model across multiple SOWs (e.g. cross categories or projects)

- **Duration and Cumulative Project or SOW Spend**

- Discounts are factored relative to a longer duration and/or higher cumulative spend across multiple SOWs for incremental project phases where there is efficiency benefits from a continuity of service (e.g. commercial strategy definition which may lead onto delivery within single or multiple categories)

- **Duration and Cumulative Overall Contract Spend**

- Multiple and cumulative SOW or projects under the overall contract value.

Schedule 2: Call-Off Contract charges

Core Services charges

The Call-Off Contract Charges for Core Services (in accordance with the Supplier's Digital Marketplace pricing document) is fixed during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term is based upon the table below.

[REDACTED]

Additional Services

1. Contract Out Services

These services are provided for on a fixed price basis and have outcome based deliverables detailed in each individual SOW.

For Contracted Out Services commissioned under the RfQ and SOW process, the SOW will detail the specific activities and milestones associated to the work and this will be used for monitoring delivery against milestones and payment. The charges for each milestone will be defined in the related in the SOW. All Contracted Out Services work packages will be priced on a fixed cost basis but the breakdown of cost per deliverable will be shown on the RFQ. The Supplier shall, where requested by the Buyer, provide a breakdown of the fixed price costs for any SOW which represents a Contracted Out Service.

The deliverables and resulting outcomes and progress will be closely monitored via weekly Buyer and Supplier governance meetings, during which the Parties may agree a change in replacement deliverables and outcomes for the next review period in line with the next milestones payment. The Parties shall review the Services and Charges in good faith to reflect any changes to the scope or cost of the Services that result from delays or material adjustments.

The Buyer Reserves the right that in the event of insufficient supporting evidence that deliverables have been achieved the buyer will issue a rectification plan to the Supplier to address this issue.

On completion of the deliverables associated with the milestones, the SOW manager will sign a Milestone Achievement Certificate which will confirm that the milestone has been delivered and payment can be authorised.

2. Resource Driven Services

These services are based on Time and Material charges for Supplier resources detailed in each individual SOW.

The Time and Material rate card that will be used for related SOWs added to this Call-off contract during the Term will be:

SFIA Level	Day rate (GBP)
SFIA Level 1	[REDACTED]
SFIA Level 2	[REDACTED]
SFIA Level 3	[REDACTED]
SFIA Level 4	[REDACTED]
SFIA Level 5	[REDACTED]

SFIA Level 6	[REDACTED]
SFIA Level 7	[REDACTED]

Standards for Consultancy Day Rate cards

- **Consultant's Working Day** – 8 hours exclusive of travel and lunch
- **Working Week** – Monday to Friday excluding national holidays
- **Outside of Working Week** – Consultants can be provided to cover non Working Week support based on the Standard Rate Card x 1.5
- **Office Hours** - 9am to 5pm Monday to Friday
- **Outside of normal Office Hours** – Consultants can be provided to cover out of Office Hours support based on the Standard Rate Card
- **Professional Indemnity Insurance** – included in day rate

Expenses

It is not anticipated that the Supplier will be required to incur travel and subsistence costs however in the event that this occurs, the Supplier shall work with the Buyer to minimise the impact on the public purse for T&S associated with the operation of this contract.

Unless otherwise provided for under the Supplier's G-Cloud 13 framework offering, and/or the Supplier has an office in close proximity to one of the Buyer's office where a meeting is to be held (approx. 25 miles radius), if expenditure on T&S is identified as being necessary, T&S will be paid at the level commensurate with the DfE rate in place at the time the expenditure is incurred. DfE rates in place as at April 2017 are listed below:

- ☐ Hotel accommodation bed and breakfast – London £110.00 including VAT and elsewhere £75.00 including VAT
- ☐ Rail travel shall be restricted to standard class
- ☐ Car mileage at the 'Public Transport Rate' of 0.25p per mile
- ☐ Taxis only payable where their use can be justified against using public transport

No other out of pocket expenses shall be allowable.

Schedule 3: Collaboration agreement – Not used

Schedule 4: Alternative clauses – Not used

Schedule 5: Guarantee – Not Used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract, or <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Change Authorisation Note (CAN)	The vehicle used to document variations made under this Call-Off-Contract in accordance with the Variation process defined in Clause 32.

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: <ul style="list-style-type: none"> • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Contracted Out Services	These services have outcome-based deliverables detailed in each individual SOW.
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
-----------------------------	-------------------------------------------------------------------------------------------


Employment Status Indicator test tool or ESI tool	<p>The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here:</p> <p>https://www.gov.uk/guidance/check-employment-status-fortax</p>
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
	defrauding or attempting to defraud or conspiring to defraud the Crown.

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

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

Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.

Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Milestone Achievement Certificate	<p>A document relating to Contracted Out Services, in the format attached, which enables the Buyer to confirm that the milestone has been achieved by the Supplier</p>  <p>Milestone Certificate Template.doc</p>
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 Services	G-Cloud	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35		Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party		The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data		Takes the meaning given in the UK GDPR.
Personal Data Breach		Takes the meaning given in the UK GDPR.
Platform		The government marketplace where Services are available for Buyers to buy.
Processing		Takes the meaning given in the UK GDPR.
Processor		Takes the meaning given in the UK GDPR.
Prohibited act		<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.

Service data	Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-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 GCloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

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

Annex 1: Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are:

[REDACTED]

Department for Education Data
Protection Officer (DPO)
2 Rivergate,
Temple Quay,
Bristol.
BS1 6ED

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

[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.

Descriptions	Details
Identity of Controller for each Category of Personal Data	The Buyer is Controller and the Supplier is Processor
Duration of the Processing	The duration of the processing commences from the contract start date and ends at the termination of the contract
Nature and purposes of the Processing	The Supplier (Processor) NTT DATA will not be able to access or view any personal data when using Service Now, DfE's incident management system. Access to this system will be for service desk call resolution only. IRIS365 full personal data is not held within the CRM element of the application which NTT DATA will not have access to or be required to modify. Limited personal data is held within CRM under the "contact card" functionality (name, post code, email address) and from Contact Us submissions (e.g. requests for information – full personal data is removed and restricted) but any

52

modifications to this element of the application would be by agreement and the RFQ process.

Type of Personal Data	Name Postcode / work location Email address Telephone number
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), Departments/ clients Contractors
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Any data will be retained for a maximum period of 3 months following termination of the contract/processing period to allow for return of the data to take place. Any held by the Processor will be returned securely electronically as directed by the DfE after which point any residual data must be destroyed following the direction of DfE security personnel

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

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

1.2 The Parties agree that the Buyer:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the Buyer's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

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

2. Undertakings of both Parties

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

- (a) report to the other Party every 3 months on: 54

- (i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
 - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
 - (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
 - (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
 - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;
- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its personnel who have access to the Personal Data and ensure that its personnel:
- (i) are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information 55

- (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;
- (iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
- (i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;
- (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance; 56

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;
and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

- (a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the contract, and procedures, including premises 57

under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant central government body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant central government body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or 58

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses; and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Not used

9. Termination

9.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (joint controller agreement), the Buyer shall be entitled to terminate the contract by issuing a termination notice to the Supplier in accordance with Clause 18.5 (Ending the contract).

10. Sub-Processing

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

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the contract, and provide evidence of such due diligence to the other Party where reasonably requested; and 59

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

11. Data Retention

11.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Annex A - DfE supplementary Conditions of Contract



CON_10981%20DfE%
20GHWT%20Tech%20

Annex A – DfE Special Clauses

Departmental Security Standards [Updated 14 December 2020]

12. Departmental Security Standards for Business Services and ICT Contracts

“BPSS”

“Baseline Personnel Security Standard”

means the Government’s HMG Baseline Personal Security Standard . Further information can be found at:

<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>

“CCSC”

“Certified Cyber Security Consultancy”

is the National Cyber Security Centre’s (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards.

See website:

<https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy>

“CCP”

“Certified Professional”

is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: <https://www.ncsc.gov.uk/information/about-certified-professional-scheme>

“CPA”

“Commercial Product Assurance”

[formerly called “CESG Product Assurance”]

is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website:

<https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>

“Cyber Essentials”

“Cyber Essentials Plus”

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.

There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers:
<https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body>
 shall have the meanings given to those terms by the Data Protection Act 2018

“Data”
 “Data Controller”
 “Data Protection Officer”
 “Data Processor”
 “Personal Data”
 “Personal Data requiring Sensitive Processing”
 “Data Subject”, “Process” and “Processing”
 “Department’s Data”
 “Department’s Information”

is any data or information owned or retained in order to meet departmental business objectives and tasks, including:
 (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:

- (i) supplied to the Contractor by or on behalf of the Department; or
- (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or
- (b) any Personal Data for which the Department is the Data Controller;

“DfE” means the Department for Education

“Department”

“Departmental Security Standards”

means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.

“Digital Marketplace / G-Cloud”

means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.

End User Devices

means the personal computer or consumer devices that store or process information.

“Good Industry Practice”

“Industry Good Practice”

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.

“Good Industry Standard”

“Industry Good Standard”

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.

“GSC”

“GSCP”

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>

“HMG”

“ICT”

means Her Majesty’s Government
 means Information and Communications Technology (ICT) and 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

“ISO/IEC 27001” “ISO 27001”

is the International Standard for Information Security Management Systems Requirements

“ISO/IEC 27002” “ISO 27002”

is the International Standard describing the Code of Practice for Information Security Controls.

"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check (ITSHC)"	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.
"IT Health Check (ITHC)"	
"Penetration Testing"	means the Need-to-Know principle 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.
"Need-to-Know"	
"NCSC"	The National Cyber Security Centre (NCSC) is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
"OFFICIAL"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP).
"OFFICIAL-SENSITIVE"	the term 'OFFICIAL-SENSITIVE' 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 GSCP.
"RBAC"	means Role Based Access Control. A method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Role Based Access Control"	
"Storage Area Network"	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"SAN"	
"Secure Sanitisation"	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
"Security and Information Risk Advisor"	The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
"CCP SIRA"	means 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
"SIRA"	
"Senior Information Risk Owner"	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SIRO"	means 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
"SPF"	
"HMG Security Policy Framework"	

12.1. The Contractor shall be aware of and comply the relevant HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

- (Guidance: Providers on the HMG Digital Marketplace / GCloud that have demonstrated compliance, as part of their scheme application, to the relevant scheme's security framework, such as the HMG Cloud Security Principles for the HMG Digital Marketplace / GCloud, may on presentation of suitable evidence of compliance be excused from compliance to similar clauses within the DfE Security Clauses detailed in this section (Section 12).)

12.2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

- (Guidance: Details of the acceptable forms of equivalence are stated at Section 9 of Annex A within the link to Cabinet Office document in this clause).
- (Guidance: The Department's expectation is that the certification scope will be relevant to the services supplied to, or on behalf of, the Department. However, where a contractor or (sub) contractor is able to evidence a valid exception or certification to an equivalent recognised scheme or standard, such as ISO 27001, then certification under the Cyber Essentials scheme could be waived. Changes to the Cabinet Office Action Note will be tracked by the DfE)
- (Guidance: The department's expectation is that SMEs or organisations of comparable size shall be expected to attain and maintain Cyber Essentials. Larger organisations or enterprises shall be expected to attain and maintain Cyber Essentials Plus.)

12.3. Where clause 12.2 above has not been met, 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).
- (Guidance: The Department's expectation is that suppliers claiming certification to ISO/IEC 27001 shall provide the Department with copies of their Scope of Certification, Statement of Applicability and a valid ISO/IEC 27001 Certificate issued by an authorised certification body. Where the provider is

able to provide a valid Cyber Essentials certification then certification under the ISO/IEC 27001 scheme could be waived and this clause may be re-moved.)

12.4. The Contractor shall follow the UK Government Security Classification Policy (GSCP) in re-spect of any Departmental Data being handled in the course of providing this service and will handle all 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 con-trols are applied to the Departmental Data).

- o (Guidance: The Department's expectations are that all contractors shall handle the Department's information in a manner compliant with the GSCP. Details of the GSCP can be found on the GOV.UK website at: <https://www.gov.uk/government/publications/government-security-classifications>.)
- o (Guidance: Compliance with the GCSP removes the requirement for the department to issue a Security Aspects Letter (SAL) to the contractor).

12.5. Departmental Data being handled in the course of providing an ICT solution or service must be separated 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 line with clause 12.14.

- o (Guidance: Advice on HMG secure sanitisation policy and approved methods are described at <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>)

12.6. The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

- o (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

12.7. The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.

- o (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

12.8. The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:

- o physical security controls;
- o good industry standard policies and processes;
- o malware protection;
- o boundary access controls including firewalls, application gateways, etc
- o maintenance and use of fully supported software packages in accordance with vendor recommendations;
- o use of secure device configuration and builds;
- o software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- o user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;

- any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
 - retained and protected from tampering for a minimum period of six months;
 - made available to the department on request.
- (Guidance: Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources or locations managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)
- (Guidance: The Minimum Cyber Security Standard issued by Cabinet Office and Information Commissioner's Office advice for the protection of sensitive and personal information recommends the use of Multi-Factor Authentication (MFA). The MFA implementation must have two factors as a minimum; with the second factor being facilitated through a separate and discrete channel, such as, a secure web page, voice call, text message or via a purpose built mobile app, such as; Microsoft Authenticator.)
- (Guidance: Further advice on appropriate levels of security audit and log collection to be applied can be found at: <https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring>.)

12.9. The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

12.10. The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.

- (Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the use of removable media as described in this clause is either prohibited or not required in order to deliver the service this clause shall be revised as follows: - 'The use of removable media in any form is not permitted'.)

12.11. The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security> and <https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles>.

- (Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

12.12. 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.

- The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".
- (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: <https://www.cpni.gov.uk/secure-destruction>)

12.13. 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

- The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

12.14. In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

- (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning sanitisation must be in accordance with guidance provided by NCSC and CPNI.

12.15. In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

- Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

- Evidence of secure destruction will be required in all cases.

- (Guidance: Where there is no acceptable secure sanitisation method available for a piece of equipment, or it is not possible to sanitise the equipment due to an irrecoverable technical defect, the storage media involved shall be destroyed using an HMG approved method described at <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>.)

- (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: <https://www.cpni.gov.uk/secure-destruction>)

- (Guidance: The term 'accounted for' means that assets and documents retained, disposed of or destroyed should be listed and provided to the department as proof of compliance to this clause.)

12.16. Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, 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 must complete this process before access to Departmental Data is permitted. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

- (Guidance: Further details of the requirements for HMG BPSS clearance are available on the website at: <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>)

- (Guidance: Further details of the requirements for National Security Vetting, if deemed necessary for this contract are available at: <https://www.gov.uk/government/publications/hmg-personnel-security-controls>)

12.17. All Contractor or sub-contractor employees who handle Departmental Data shall have an annual awareness training in protecting information.

12.18. 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.

- o (Guidance: The business continuity and disaster recovery plans should be aligned with industry good practice and it is the Department's expectation that all vendors providing services or infrastructure to the Department will have plans that are aligned to the ISO 22301 standard in place. Further information on the requirements of ISO 22301 may be found in the standard.)

12.19. Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution

- o Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.
- o Incidents shall be reported through the department's nominated system or service owner.
- o Incidents shall be investigated by the contractor with outcomes being notified to the Department.

12.20. 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 an NCSC CHECK Scheme 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.

- o (Guidance: Further information on IT Health Checks and the NCSC CHECK Scheme which enables penetration testing by NCSC approved companies can be found on the NCSC website at: <https://www.ncsc.gov.uk/scheme/penetration-test-ing>.)

12.21. The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

- o (Guidance: The offshoring of HMG information outside of the UK is subject to approval by the Departmental SIRO).

12.22. The Department reserves the right to audit the Contractor or sub-contractors 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.

12.23. The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. 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 Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

- (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning their organisation. Further advice and guidance on the Department's security assurance processes can be supplied on request. Information about the HMG Supplier Assurance Framework can be found at: <https://www.gov.uk/government/publications/government-supplier-assurance-framework>

- (Guidance: Further information on the CCP and CCSC roles described above can be found on the NCSC website at: <https://www.ncsc.gov.uk/information/about-certified-professional-scheme> and <https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy>)

12.24. Where the Contractor is delivering an ICT solution to the Department they shall design and 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:

- Compliance with HMG Minimum Cyber Security Standard.

- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.

- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

- 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.

12.25. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

Other clauses:

Modern Slavery, Child Labour and Inhumane Treatment

1.1 The Contractor:

1.1.1 shall not use, or allow its Subcontractors to use, forced, bonded or involuntary prison labour;

1.1.2 shall not require any Contractor staff or Subcontractor staff to lodge deposits or identify papers with the Employer or deny Contractor staff freedom to leave their employer after reasonable notice;

1.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

1.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.

1.1.5 shall make reasonable enquiries to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world.

1.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and shall include in its contracts with its subcontractors anti-slavery and human trafficking provisions;

1.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

1.1.8 shall prepare and deliver to the Department at the commencement of each Contract and updated on a frequency defined by the Department, a slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business;

1.1.9 shall not use, or allow its employees or Subcontractors to use, physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

1.1.10 shall not use, or allow its Subcontractors to use, child or slave labour; 70

1.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to the Department and Modern Slavery Helpline¹.

¹ The "Modern Slavery Helpline" refers to the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at <https://www.modernslaveryhelpline.org/report> or by telephone on 08000 121 700.

Annex B - RfQ Template



RFQ%20Template%
20v7.8%20Blank%20

Annex C – Monthly Service Report Template



Master%20service%
20report%20-%20Fe

Annex D – Milestone achievement certificate



Milestone Certificate
Template.doc