

## G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

### G-Cloud 14 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	16
Schedule 1: Services	37
Schedule 2: Call-Off Contract charges	40
Schedule 3: Collaboration agreement	45
Schedule 4: Alternative clauses	46
Schedule 5: Guarantee	47
Schedule 6: Glossary and interpretations	48
Schedule 7: UK GDPR Information	62
Annex 1: Processing Personal Data	62
Annex 2: Joint Controller Agreement	64
Schedule 8: Corporate Resolution Planning	65
Annex 1: Department for Education Special Conditions for Contract	82
Schedule 9: Variation Form	95

## 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.

<b>Platform service ID number</b>	409708968340057
<b>Call-Off Contract reference</b>	Con_26329
<b>Call-Off Contract title</b>	<b>Data Standards in Children's Social Care</b>
<b>Call-Off Contract description</b>	Cloud based service providing support for the 3-year programme of delivery to define, evidence and prioritise use cases (Year 1), develop agreed data standards (Year 2) and launch standards to the sector (Year 3).
<b>Start date</b>	17 <sup>th</sup> January 2025
<b>Expiry date</b>	16 <sup>th</sup> January 2028  <b>3 years plus optional +1 extension (with extension to 16/01/29)</b>
<b>Call-Off Contract value</b>	£3,393,125 (£4,071,750 inc. vat)  <b>plus, optional 12-month extension at £1,131,041 = total £4,524,166 (£5,428,999)</b>
<b>Charging method</b>	BACS
<b>Purchase order number</b>	To be issued post contract award

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

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.

<b>From the Buyer</b>	The Secretary of State for the Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
<b>To the Supplier</b>	Social Finance Ltd 87 Vauxhall Walk, London SE11 5HJ  Company number: 06402143
<b>Together the 'Parties'</b>	

## Principal contact details

### For the Buyer:

Title: Contract and Delivery Manager

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

### For the Supplier:

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

## Call-Off Contract term

<b>Start date</b>	This Call-Off Contract Starts on <b>17<sup>th</sup> January 2025</b> and is valid for <b>3 years</b> .
-------------------	--

<b>Ending (termination)</b>	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least <b>90</b> 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 <b>30</b> days from the date of written notice for Ending without cause (as per clause 18.1).</p>
<b>Extension period</b>	<p>This Call-Off Contract can be extended by the Buyer for <b>one</b> period of up to 12 months, by giving the Supplier <b>4 weeks</b> 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> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p><a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a></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.

<b>G-Cloud Lot</b>	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> <li>● Lot 3: Cloud support</li> </ul>
<b>G-Cloud Services required</b>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <p><input type="checkbox"/> Ref 2.5.10 - information and communication technology (ICT)</p>

	See Schedule 1 (Services) for the maximum anticipated volumes of all services under this Call-Off Contract although there is no guarantee to the Supplier of volume.
<b>Additional Services</b>	Any additional related G Cloud services the Supplier can provide through the Digital Marketplace may be required and will be subject to a specification and financial proposal provided by the Supplier and approved by the Buyer.
<b>Location</b>	The Services will be delivered remotely.
<b>Quality Standards</b>	The quality standards required for this Call-Off Contract are detailed in the Service Standard <a href="http://www.gov.uk">Service Standard - Service Manual - GOV.UK (www.gov.uk)</a>
<b>Technical Standards:</b>	See Service Standard above
<b>Service level agreement:</b>	The service level and availability criteria required for this Call-Off Contract are included as part of the <b>Performance of the Service and Deliverables</b> below
<b>Onboarding</b>	N/A – new requirement and contract

<b>Offboarding</b>	<p>The offboarding plan for this Call-Off Contract is:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Any Intellectual Property (IP) created during or for this work package is owned by the Department for Education.</li> <li><input type="checkbox"/> Dedicated handover time so DfE understand how to use the standards/ what technical skills are required if any (to be considered as part of the exit plan)</li> </ul> <p>Further offboarding agreements will be documented in the exit plan.</p>
<b>Collaboration agreement</b>	Not applicable

<b>Limit on Parties' liability</b>	<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 £1,000,000 per year.</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 £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
<b>Buyer's responsibilities</b>	N/A
<b>Buyer's equipment</b>	N/A
<b>Insurance</b>	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>• a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</li> <li>• 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 aggregate limit of indemnity of £5,000,000 or any higher limit the Buyer requires (and as required by Law)</li> <li>• employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law</li> </ul>
<b>Force majeure</b>	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
<b>Audit</b>	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 as required from clauses 7.4 to 7.13 of the Framework Agreement.

## Supplier's information

<b>Subcontractors or partners</b>	The following is a list of the Supplier's Subcontractors or Partners : Open Data Institute Coram Individual consultants: <b>[REDACTED]</b> , <b>[REDACTED]</b> , <b>[REDACTED]</b>
-----------------------------------	---




## 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.

<b>Payment method</b>	The payment method for this Call-Off Contract is <b>BACS</b>
<b>Payment profile</b>	The payment profile for this Call-Off Contract is <b>monthly</b> in arrears.
<b>Invoice details</b>	The Supplier will issue electronic invoices <b>monthly</b> in arrears. The Buyer will pay the Supplier within <b>30</b> days of receipt of a valid invoice.
<b>Who and where to send invoices to</b>	Accounts Payable, ASC Purchasing, Cheylesmore House, Quinton Road, Coventry, CV1SWT <a href="mailto:accountspayable.ocr@education.gov.uk">accountspayable.ocr@education.gov.uk</a> cc: <b>[REDACTED]</b> <u>and</u> <b>[REDACTED]</b>
<b>Invoice information required</b>	All invoices must include <ul style="list-style-type: none"><li>• Project reference number</li><li>• SoW reference number</li><li>• Purchase order number</li><li>• Description of charges</li><li>• Dates for the charges invoiced</li></ul>

<b>Invoice frequency</b>	Invoice will be sent to the Buyer Monthly.
<b>Call-Off Contract value</b>	<p>The total value of this Call-Off Contract is £3,393,125 (£4,071,750 inc vat)</p> <p><b>plus, optional 12-month extension at £1,131,041 = total £4,524,166 (£5,428,999)</b></p>
<b>Call-Off Contract charges</b>	<p>The breakdown of the Charges is:</p> <p><b>[REDACTED]</b></p> <p><b>[REDACTED]</b></p>
<b>Statement of Work Approach</b>	<p>This call-off contract will use a Statement of Work (SOW) approach.</p> <p>All deliverables, acceptance criteria, timelines and costs will be set out in each Statement of Work (SoW). SoWs will be agreed and signed by both parties before commencement of work. Service credits may be applied and outlined within individual work packages.</p> <p>Any additional services as listed in the Suppliers Service Description will be agreed through a SOW process in agreement with the buyer and supplier.</p> <p>The supplier will meet 100% of Key Milestones and Key Deliverables (for which it is responsible) to the agreed dates, as set out in each SOW. A Key Milestone or Key Deliverable will not be defined as missed if an exception is agreed with the Buyer's Principal Contact in</p>




	<p>advance or the Key Milestone or Key Deliverable is not the responsibility of the Supplier.</p> <p>The Statement of Work and Change Control Notice templates are attached</p> <div style="display: flex; justify-content: space-around; align-items: center;">    </div> <p style="text-align: center;">             Outside IR35 -      DfE SOW Change      Statement of Work              Statement of Work TControl Notice Temp      Template v1.4 TA - Ins         </p>
--	--


## Additional Buyer terms

<b>Performance of the Service</b>	This Call-Off Contract will include the KPIs and SLAs as detailed in the attached document:				
	<b>KPI Reference</b>	<b>Service Level Performance Criterion</b>	<b>Key Indicator</b>	<b>Service Level Performance Measure</b>	<b>Service Level Threshold</b>
	KPI001	<b>Service Timeliness</b>	95% of services required by the Supplier to deliver the outcomes agreed and commence work on the date agreed with the Authority. Services are defined as the individuals who will be performing services in relation to the agreed work package.	<b>Good</b> – 95% or above of services required commence work on agreed date. <b>Approaching Target</b> – 90-95% of services required commence work on agreed date. <b>Requires Improvement</b> – 80-90% of services required commence work on agreed date. <b>Inadequate</b> – <80% of services required	The service level measure is 'Good' across a 3-month period.

			commence work on agreed date. Subject to all SOW's over a 3-month period.	
KPI002	<b>Quality of service/ individuals provided to deliver outcomes agreed</b>	<p>Number of Services provided by the Supplier have the appropriate skills and experience required to deliver the outcomes agreed between Authority and Supplier.</p> <p>This will be measured through the number of individuals being swapped out due to the Supplier not meeting the outcomes/milestones agreed or where the customer has formally complained in writing with performance levels.</p>	<p><b>Good</b> – 0 personnel swap-outs across the SOW period.</p> <p><b>Approaching Target</b> – 1 personnel swap-outs across the SOW period.</p> <p><b>Requires Improvement</b> – &lt;3 personnel swap-outs across the SOW period.</p> <p><b>Inadequate</b> – 3&gt; swap-outs across the SOW period. Subject to all active SOW's over a monthly period.</p>	The service level measure is ' <b>Good</b> ' across a monthly period.
KPI003	<b>Invoice accuracy</b>	<p>Invoices submitted in the Measurement Period are correct.</p> <p>Definition:</p> <ul style="list-style-type: none"> <li>- Invoice does not overlap with previous invoice period.</li> <li>- Services and rates align with those agreed on prevailing SoW.</li> <li>- <b>Purchase order quoted is correct.</b></li> <li>- Invoice does not bill for services not rendered.</li> <li>- Invoice does not bill for outcomes which have not been delivered.</li> <li>- Invoice does not bill for expenses which have not been approved (in writing) by the Authority.</li> <li>- Any expenses billed for must comply with the Authorities expenses policy.</li> </ul>	<p><b>Good</b> – 100% of invoices are accepted.</p> <p><b>Approaching Target</b> – 90% of invoices are accepted.</p> <p><b>Requires Improvement</b> – 80% of invoices are accepted.</p> <p><b>Inadequate</b> – &lt;80% of invoices are accepted.</p>	The service level measure is 'Approaching Target' across a quarterly period.

	KPI004	Successful delivery of outcomes and acceptance criteria against milestone dates.	The supplier delivers the outcomes agreed in each work package in line with the acceptance criteria and milestone dates.	<b>Good</b> – 90%> of outcomes delivered and accepted by Authority. <b>Approaching Target</b> – 80% of outcomes delivered and accepted by Authority. <b>Requires Improvement</b> – 70% of outcomes delivered and accepted by Authority. <b>Inadequate</b> – <70% of outcomes delivered and accepted by Authority.	The service level measure is 'Good' across a quarterly period.
	KPI005	The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the EIR	<p>1. Provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and EIR;</p> <p>1.2 transfer to the Authority all requests for information relating to the Contract that it receives as soon as practicable and in any event within 2 Working Days of receipt;</p> <p>1.3 provide the Authority with a copy of all Information belonging to the Authority requested which is in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may reasonably specify) of the Authority's request for such information; and</p> <p>1.4 not respond directly to a request for information unless authorised in writing to do so by the Authority.</p> <p>2 The Supplier acknowledges that the Authority may be required</p>		

	<table><tr><td></td><td></td><td>under the FOIA and EIR to disclose Information (including Confidential Information) without consulting or obtaining consent from the Supplier. The Authority shall take reasonable steps to notify the Supplier of a request for information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in the Contract) the Authority shall be responsible for determining in its absolute discretion whether any Confidential Information and/or any other information is exempt from disclosure in accordance with the FOIA and/or the EIR.</td><td></td><td></td></tr></table>			under the FOIA and EIR to disclose Information (including Confidential Information) without consulting or obtaining consent from the Supplier. The Authority shall take reasonable steps to notify the Supplier of a request for information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in the Contract) the Authority shall be responsible for determining in its absolute discretion whether any Confidential Information and/or any other information is exempt from disclosure in accordance with the FOIA and/or the EIR.		
		under the FOIA and EIR to disclose Information (including Confidential Information) without consulting or obtaining consent from the Supplier. The Authority shall take reasonable steps to notify the Supplier of a request for information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in the Contract) the Authority shall be responsible for determining in its absolute discretion whether any Confidential Information and/or any other information is exempt from disclosure in accordance with the FOIA and/or the EIR.				
Guarantee	Not required					
Warranties, representations	Not required					
Supplemental requirements in addition to the Call-Off terms	<p>Within the scope of the Call-Off Contract, the Supplier will:</p> <p>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 [Enter] (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.</p> <div><p>HMG_Baseline_Perso nnel_Security_Standar</p></div>					

	<p>2. The Supplier terms attached for convenience</p> <p>3. The Supplier agrees to the variations below to the Buyer standard clauses in respect of Information Security requirements, also attached at Annex A:</p> <p></p> <p>Annex%20A_Buyer%20Security%20Standards</p>
<b>Alternative clauses</b>	Not applicable
<b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b>	<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"> <li>• G-Cloud 14 Framework Agreement</li> <li>• G-Cloud 14 Order Form</li> <li>• G-Cloud 14 Call-Off Contract</li> <li>• Buyer Supplemental Security clauses and Conditions of Contract (Annex A)</li> <li>• Supplier Terms and Conditions</li> </ul> <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>
<b>Personal Data and Data Subjects</b>	See Schedule 7, Annex 1
<b>Intellectual Property</b>	Any Intellectual Property (IP) created throughout this call-off contract and any specific work packages is owned by the Department for Education.
<b>Social Value</b>	<p><b>SOCIAL VALUE:</b> please explain the effective measures to deliver any/all the following benefits through the contract:</p> <ul style="list-style-type: none"> <li>• create opportunities for entrepreneurship and help new organisations to grow, supporting economic growth and business creation</li> <li>• create employment and training opportunities particularly for those who face barriers to employment and/or who are in deprived areas, and for people in industries with known skills shortages or in high growth sectors</li> <li>• support educational attainment relevant to the contract, including training schemes that address skills gaps and result in recognised qualifications.</li> </ul> <p>Create opportunities for entrepreneurship and help new organisations to grow, supporting economic growth and business creation - The project will work with Social Finance's innovation support partnerships network, which supports a range of tech companies to innovate and grow, to identify opportunities for these entrepreneurs to develop data and digital solutions that can support DfE and Local Authorities improve their use of data. We will invite relevant and interested SMEs and entrepreneurs to a "brown bag lunches" where we speak through non-confidential aspects of the project enabling them to propose solutions that will assist DfE and LAs in improving data use in CSC. We will provide a summary of ideas and suggestions and submit to DfE. Subject to further funding we will engage further with DfE and the entrepreneurs to develop these ideas into workable solutions.</p> <p>Create employment and training opportunities particularly for those who face barriers to employment and/or who are in deprived areas, and for people in industries with known skills shortages or in high growth sectors - Leveraging Social Finance's extensive expertise in the employment sector (e.g. Mental Health and Employment Partnerships), we will ensure the project aligns with our commitment to a diverse and representative workforce internally and among our partners, and embeds approaches to building skills and tackling barriers to employment. Across all our projects we promote equality within our workforce by adopting a flexible working culture (e.g. working hours, remote working) that enables staff from all backgrounds and from across the country to join our team. We've worked to reduce bias in our recruitment process by anonymising the initial phase, and provide apprenticeship opportunities and an extensive training curriculum to support accessible routes into our workforce. To ensure accountability for tackling inequality, we've established an independent Race Equity Advisory Group, we proactively train managers in leading a diverse organisation, and provide an "Unlearning Racism" programme to support our team in becoming actively anti-racist.</p> <p>Support educational attainment relevant to the contract, including training schemes that address skills gaps and result in recognised qualifications - Having worked with Data 2 Insight to develop and deliver a data apprenticeship in Children's Social Care, training 91 people in total, SF understand the value, and the challenges, of addressing skills gaps within Local Authorities in this area. Under this contract, in our engagements with local authorities, we will seek an updated view of the value of apprenticeships and consider whether this is a vehicle which can be used to (1) expand further the skills of the current workforce through recognised qualifications, and (2) whether it can be used to aid recruitment to expand and develop the data workforce across LAs in CSC. We will do this through initial light touch engagement, followed by more intensive discussion if needed - and potentially the leveraging of the apprenticeship levy to support further work in this area.</p>

<b>Performance Indicators</b>	Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.
-------------------------------	---

## 1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive 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 RM1557.14.

<b>Signed</b>	Supplier	Buyer
<b>Name</b>	[REDACTED]	[REDACTED]
<b>Title</b>	Interim CEO	Commercial Lead
<b>Signature</b>	[REDACTED]	[REDACTED]
<b>Date</b>	17 <sup>th</sup> January 2025	17 <sup>th</sup> January 2025

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

## Buyer Benefits

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

[G-Cloud 14 Buyer 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 36 months.

### 2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses, schedules 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)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (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)
- 30 (Insurance)



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

## 5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
  - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
  - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
  - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
  - 5.1.4 have entered into the Call-Off Contract relying on 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 aggregate limit £5,000,000 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

## 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 trademarks 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 judgement 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-security-classifications>

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

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

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

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



13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

## 14. Standards and quality

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

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

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 CDDO 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 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

- 23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.
- 23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

## 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 is not a Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

## 28. Environmental requirements

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

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

## 29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
  - 29.2.2 age
  - 29.2.3 start date
  - 29.2.4 place of work
  - 29.2.5 notice period
  - 29.2.6 redundancy payment entitlement
  - 29.2.7 salary, benefits and pension entitlements
  - 29.2.8 employment status
  - 29.2.9 identity of employer
  - 29.2.10 working arrangements
  - 29.2.11 outstanding liabilities
  - 29.2.12 sickness absence
  - 29.2.13 copies of all relevant employment contracts and related documents
  - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.
- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

- 29.5 The Supplier will cooperate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
- 29.6.1 its failure to comply with the provisions of this clause
  - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

### 30. Additional G-Cloud services

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

### 31. Collaboration

- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
- 31.2.1 work proactively and in good faith with each of the Buyer's contractors
  - 31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

## 32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 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 using the template in Schedule 9. This includes any changes in the Supplier's supply chain.
- 32.3 If either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days' notice to the Supplier.

## 33. Data Protection Legislation (GDPR)

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

# Schedule 1: Services

Lot 2: Cloud support

## **Social Finance Data and Digital Innovation Service**

Social Finance works with partners, people and communities to identify problems and pain points, co-design and deliver cloud-based products and services that deliver better services and outcomes.

### **Features**

- user-centred research and design
- cloud-based tech strategy
- service, systems and architecture requirements mapping
- service and organisational design
- change, transformation and implementation support
- system design
- capacity-building and training
- prototyping of cloud-based products and services
- design, build and maintain cloud-based products and services
- UI/UX design

### **Benefits**

- improved outcomes for people and communities
- user-centred services that meet users' needs
- co-designed products and services with users and staff
- improved capacity and knowledge
- implementable roadmap for cloud-based infrastructure, products and services
- cost-effective cloud-based products and services
- services and organisations re-designed to improve experiences of people
- business analysis and cost benefit analysis to unlock funding
- products and services that integrate with legacy systems and skillsets
- robust measurement and monitoring of outcomes

# Services Overview

KEY FEATURES	KEY BENEFITS
<ul style="list-style-type: none"><li>• User-centred research and design</li><li>• Cloud-based tech strategy</li><li>• Service, systems and architecture requirements mapping</li><li>• Service and organisational design</li><li>• Change, transformation and implementation support</li><li>• System design</li><li>• Capacity-building and training</li><li>• Prototyping of cloud-based products and services</li><li>• Design, build and maintain cloud-based products and services</li><li>• UI/UX design</li></ul>	<ul style="list-style-type: none"><li>• Improved outcomes for people and communities</li><li>• User-centred services that meet users' needs</li><li>• Co-designed products and services with users and staff</li><li>• Improved capacity and knowledge</li><li>• Implementable roadmap for cloud-based infrastructure, products and services</li><li>• Cost-effective cloud-based products and services</li><li>• Services and organisations re-designed to improve experiences of people</li><li>• Business analysis and cost benefit analysis to unlock funding</li><li>• Products and services that integrate with legacy systems and skillsets</li><li>• Robust measurement and monitoring of outcomes</li></ul>

## How the planning service works

Social Finance has designed, built and scaled cloud-based products and services.

We use user research, service design, organisation design, technical expertise (full-stack) and transformation support to enable partners to plan, design, embed and scale cloud-based products and services.

We can support partners design, build, and scale cloud-based solutions through:

- Business analysis
- Data analysis
- User research and service and organisation design to inform products and services
- Prototyping (low to high fidelity) cloud-based solutions
- Product and solution design and implementation
- Mapping existing infrastructure and making infrastructure recommendations
- Service blueprints
- Developing Cloud software and hosting business cases
- Assessment of organisational or team capability and skill and readiness
- Assessment (tech, service, cost benefit) of cloud based products and vendors

## How the training service works

Training and capacity core to our offer to partners. We've in-depth skills and experiences to support partners through training and support:

- Working alongside teams/individuals to upskill
- Workshops and micro-trainings (user research, service design, serverless, vision setting, strategy sessions, etc)
- Knowledge and capability training through paired working
- Coaching on designing and delivering implementation strategies

## Schedule 2: Call-Off Contract charges

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

The breakdown of the Charges is:

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

### Total charge over 36 + 12 optional extension months

Annual service charge:

Year 1 = [REDACTED]

Year 2 = [REDACTED]

Year 3 = [REDACTED]

Optional Year 4 Extension = [REDACTED]

Total service charge for 36 months + 12 optional extension months = [REDACTED] = total  
[REDACTED] (£[REDACTED])



## Call-Off Contract Pricing Schedule

### **Year 1 Pricing Schedule**

[REDACTED]

### **Year 2 Pricing Schedule**

[REDACTED]

### **Year 3 Pricing Schedule**

[REDACTED]

### ***Year 4 Optional Pricing Schedule of extension***

Any work agreed in year 4 will be using SoWs with the existing agreed pricing schedule.

## Schedule 3: Collaboration agreement

Not Applicable

## Schedule 4: Alternative clauses

See Annex A below

## Schedule 5: Guarantee

Not Applicable

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses.
<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"><li>• 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</li><li>• created by the Party independently of this Call-Off Contract, or</li></ul> <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>
<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.

<b>Buyer Software</b>	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.
<b>Call-Off Contract</b>	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.
<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	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.
<b>Commercially Sensitive Information</b>	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.
<b>Confidential Information</b>	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

<b>Controller</b>	Takes the meaning given in the UK GDPR.
<b>Crown</b>	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.
<b>Data Loss Event</b>	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.
<b>Data Protection Impact Assessment (DPIA)</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
<b>Data Protection Legislation (DPL)</b>	(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.
<b>Data Subject</b>	Takes the meaning given in the UK GDPR
<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• 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</li> </ul> <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>
<b>DPA 2018</b>	Data Protection Act 2018.

<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	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.
<b>Equipment</b>	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.
<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	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: <a href="https://www.gov.uk/guidance/check-employment-status-fortax">https://www.gov.uk/guidance/check-employment-status-fortax</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.
<b>Financial Metrics</b>	The following financial and accounting measures: <ul style="list-style-type: none"> <li>• Dun and Bradstreet score of 50</li> <li>• Operating Profit Margin of 2%</li> <li>• Net Worth of 0</li> <li>• Quick Ratio of 0.7</li> </ul>



<b>Force Majeure</b>	<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"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• 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</li> <li>• the event was foreseeable by the Party seeking to rely on Force</li> </ul> <p>Majeure at the time this Call-Off Contract was entered into</p> <ul style="list-style-type: none"> <li>• 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</li> </ul>
<b>Former Supplier</b>	<p>A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).</p>
<b>Framework Agreement</b>	<p>The clauses of framework agreement RM1557.14 together with the Framework Schedules.</p>
<b>Fraud</b>	<p>Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.</p>
<b>Freedom of Information Act or FoIA</b>	<p>The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or</p>

	codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
<b>G-Cloud Services</b>	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.
<b>UK GDPR</b>	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
<b>Good Industry Practice</b>	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.
<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	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.
<b>Implementation Plan</b>	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.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information security management system</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.

<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
<b>Insolvency event</b>	Can be: <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> <li>• a Supplier Trigger Event</li> </ul>
<b>Intellectual Property Rights or IPR</b>	Intellectual Property Rights are: (a) 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 (b) 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 • (c) all other rights having equivalent or similar effect in any country or jurisdiction
<b>Intermediary</b>	For the purposes of the IR35 rules an intermediary can be: <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul> It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
<b>IPR claim</b>	As set out in clause 11.5.
<b>IR35</b>	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.
<b>IR35 assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
<b>Know-How</b>	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.

<b>Law</b>	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, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	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.
<b>Management Charge</b>	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.
<b>Management Information</b>	The management information specified in Framework Agreement Schedule 6.
<b>Material Breach</b>	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.
<b>Ministry of Justice Code</b>	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.

<b>New Fair Deal</b>	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.
<b>Order</b>	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.
<b>Performance Indicators</b>	The performance information required by the Buyer from the Supplier set out in the Order Form.
<b>Personal Data</b>	Takes the meaning given in the UK GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the UK GDPR.
<b>Platform</b>	The government marketplace where Services are available for Buyers to buy.
<b>Processing</b>	Takes the meaning given in the UK GDPR.
<b>Processor</b>	Takes the meaning given in the UK GDPR.

<b>Prohibited act</b>	<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"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
<b>Project Specific IPRs</b>	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.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	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.
<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	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.

<b>Relevant person</b>	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.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.
<b>Replacement Services</b>	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.
<b>Replacement supplier</b>	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).
<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Service Data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
<b>Service definition(s)</b>	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.
<b>Service description</b>	The description of the Supplier service offering as published on the Platform.
<b>Service Personal Data</b>	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.

<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
<b>Subcontractor</b>	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.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
<b>Supplier staff</b>	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.
<b>Supplier Terms</b>	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.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.



<b>Trigger Event</b>	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).
<b>Variation Impact Assessment</b>	<p>An assessment of the impact of a variation request by the Buyer completed in good faith, including:</p> <ul style="list-style-type: none"> <li>a) details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract;</li> <li>b) details of the cost of implementing the proposed variation;</li> <li>c) details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;</li> <li>d) a timetable for the implementation, together with any proposals for the testing of the variation; and</li> </ul> <p>such other information as the Buyer may reasonably request in (or in response to) the variation request;</p>
<b>Working Days</b>	Any day other than a Saturday, Sunday or public holiday in England and Wales.
<b>Year</b>	A contract year.

Intentionally Blank

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

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p><b>The Buyer is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller, and the Supplier is the Processor of the following Personal Data recorded below:</p> <p>Names and contact details of any stakeholders involved over the course of the project, e.g. interview partners/ workshop participants/ user groups/ advisory group members</p>
Duration of the Processing	Processing will be for the length of the contract from commencement date (17 January 2025) to end date (16 January 2027, or 16 January 2028 if the optional extension is exercised)
Nature and purposes of the Processing	<p>Processing data in order to deliver the service the customer has requested in-line with the G-Cloud 14 service offering.</p> <p>The nature and purpose of processing is to facilitate collection of personal data and provide NCS specific advice around education and career pathways. The reasons the customer is contacting the National Careers Service vary e.g., seeking general career advice requesting details on a specific training course or apprenticeship.</p> <p>This would include:</p> <p>Collection, Recording, Organisation, Structuring, Storage, Use, Disclosure by transmission, Dissemination, Combination, Erasure, Destruction (Manual or Automated), Retrieval, Consultation and for the purpose of the maintenance, support and continuous improvement of National Careers Service data services</p>

Type of Personal Data	<p>Personally identifiable information and personal sensitive information including but not limited to;</p> <ul style="list-style-type: none"> <li>o Name;</li> <li>o date of birth / age;</li> <li>o postal address;</li> <li>o email address;</li> <li>o telephone number(s);</li> </ul>
Categories of Data Subject	<p>Data Subjects of the Personal Data referred to above, which may include:</p> <p>(a) Staff (including volunteers, agents, and temporary workers) of the Relevant Authority. (b) Members of the public who are using the National Careers Service:</p> <ul style="list-style-type: none"> <li>(i) Under the age of 16</li> <li>(ii) Over the age of 16</li> </ul>
International transfers and legal gateway	<p><b>Personal data will be stored in the UK and only accessed from the UK .</b></p> <ul style="list-style-type: none"> <li>• <i>We have configured our Microsoft service to host all data in the UK</i></li> <li>• <i>We also have a 'geographic block' configured which means that even our own staff cannot log in from outside the UK unless IT specifically unblock them, and we have a process to ensure this is only used appropriately.</i></li> <li>• <i>Staff are not allowed to store personal data locally, or on removable media, we have automated systems to detect unusual downloads</i></li> </ul>
Plan for return and destruction of the data once the Processing is complete	<p>The records will be security destroyed once the processing is complete, and a destruction certificate provided, or the records will be returned to the Department and the records permanently withdrawn from the IT database</p> <p>All data will be erased from the IT system within 12 months of expiry of contract and a destruction certificate provided.</p>

## Annex 2 - Joint Controller Agreement

Not Applicable

## Schedule 8 (Corporate Resolution Planning)

### 1. Definitions

- 1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

<b>"Accounting Reference Date"</b>	means in each year the date to which the Supplier prepares its annual audited financial statements;
<b>"Annual Revenue"</b>	<p>means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:</p> <p>figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and</p> <p>where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to</p>

	British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
<b>“Appropriate Authority” or “Appropriate Authorities”</b>	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
<b>“Associates”</b>	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
<b>"Cabinet Office Markets and Suppliers Team"</b>	means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;

<b>“Class 1 Transaction”</b>	has the meaning set out in the listing rules issued by the UK Listing Authority;
<b>“Control”</b>	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
<b>“Corporate Change Event”</b>	<p>means:</p> <ul style="list-style-type: none"> <li>(a) any change of Control of the Supplier or a Parent Undertaking of the Supplier;</li> <li>(b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;</li> <li>(c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;</li> <li>(d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;</li> <li>(e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;</li> </ul>



	<p>(f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;</p> <p>(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;</p> <p>(h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;</p> <p>(i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or</p> <p>(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;</p>
<b>"Corporate Change Event Grace Period"</b>	means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;

<p><b>"Corporate Resolvability Assessment (Structural Review)"</b></p>	<p>means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;</p>
<p><b>"Critical National Infrastructure" or "CNI"</b></p>	<p>means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>significant impact on the national security, national defence, or the functioning of the UK;</p>
<p><b>"Critical Service Contract"</b></p>	<p>means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;</p>

<p><b>“CRP Information”</b></p>	<p>means the corporate resolution planning information, together, the:</p> <p>(a) Exposure Information (Contracts List);</p> <p>(b) Corporate Resolvability Assessment (Structural Review); and</p> <p>(c) Financial Information and Commentary</p>
<p><b>“Dependent Parent Undertaking”</b></p>	<p>means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;</p>
<p><b>“FDE Group”</b></p> <p><b>“Financial Distress Event”</b></p>	<p>means the [Supplier, Subcontractors, [the Guarantor]</p> <p>the credit rating of an FDE Group entity dropping below the applicable Financial Metric;</p>

	<p>an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;</p> <p>there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;</p> <p>an FDE Group entity committing a material breach of covenant to its lenders;</p> <p>a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;</p> <p>any of the following:</p> <p>commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;</p> <p>non-payment by an FDE Group entity of any financial indebtedness;</p> <p>any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;</p> <p>the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity;</p> <p>or</p> <p>the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;</p> <p>in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and</p> <p>any two of the Financial Metrics for the Supplier not being met at the same time.</p>
--	---

<b>“Parent Undertaking”</b>	has the meaning set out in section 1162 of the Companies Act 2006;
<b>“Public Sector Dependent Supplier”</b>	means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
<b>“Strategic Supplier”</b>	means those suppliers to government listed at <a href="https://www.gov.uk/government/publications/strategic-suppliers">https://www.gov.uk/government/publications/strategic-suppliers</a> ;
<b>“Subsidiary Undertaking”</b>	has the meaning set out in section 1162 of the Companies Act 2006;
<b>“Supplier Group”</b>	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;

<b>“UK Public Sector Business”</b>	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and
<b>“UK Public Sector / CNI Contract Information”</b>	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;

## 2. Service Status and Supplier Status

2.1 This Call-Off Contract is not a Critical Service Contract.

The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is [resolution.planning@cabinetoffice.gov.uk](mailto:resolution.planning@cabinetoffice.gov.uk).

2.2 The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer's rights under this Schedule.

### 3. Provision of Corporate Resolution Planning Information

- 3.1 Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.
- 3.2 Subject to Paragraphs 3.6, 3.10 and 3.11:
  - 3.2.1 where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and
  - 3.2.2 except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.
- 3.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

3.3.1 is full, comprehensive, accurate and up to date;

3.3.2 is split into three parts:

- (a) Exposure Information (Contracts List);
- (b) Corporate Resolvability Assessment (Structural Review);
- (c) Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

3.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

3.3.4 provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and

3.3.5 complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

3.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the



Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

3.5 If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

3.5.1 the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

3.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

3.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

3.7 An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

- 3.7.1 the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and
  - 3.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.
- 3.8 If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:
- 3.8.1 within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11) unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;
  - 3.8.2 within 30 days of a Corporate Change Event unless
    - (a) the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and

the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

- (b) not required pursuant to Paragraph 3.10;

3.8.3 within 30 days of the date that:

- (a) the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or
- (b) none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

3.8.4 in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

- (a) updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or
- (b) not required pursuant to Paragraph 3.10.

- 3.9 Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.
- 3.10 Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

3.10.1 Aa3 or better from Moody's;

3.10.2 AA- or better from Standard and Poors;

3.10.3 AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

- 3.11 Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

## 4. Termination Rights

4.1 The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

- 4.1.1 the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or
- 4.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

## 5. Confidentiality and usage of CRP Information

- 5.1 The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.
- 5.2 Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms

no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.

- 5.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.
- 5.4 Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

- 5.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;
- 5.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:

- (a) summarising the information;
- (b) grouping the information;
- (c) anonymising the information; and
- (d) presenting the information in general terms

- 5.5 The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

# ANNEX A: Department for Education Special Conditions for Contract

## Departmental Security Requirements [Updated 14 December 2023]

### Departmental Security Standards for Business Services and ICT Contracts

#### 1. Definitions

- 1.1. In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

“BPSS” “Baseline Personnel Security Standard”	the Government’s HMG Baseline Personal Security Standard. Further information can be found at: <a href="https://www.gov.uk/government/publications/government-baseline-personnel-security-standard">https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</a>
“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: <a href="https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy">https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy</a>
“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: <a href="https://www.ncsc.gov.uk/information/about-certified-professional-scheme">https://www.ncsc.gov.uk/information/about-certified-professional-scheme</a>

<p>“Cyber Essentials” “Cyber Essentials Plus”</p>	<p>Cyber Essentials is the government backed industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme, the link below points to these providers:</p> <p><a href="https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body">https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body</a></p>
<p>“Data” “Data Controller” “Data Protection Officer” “Data Processor” “Personal Data” “Personal Data requiring Sensitive Processing” “Data Subject”, “Process” and “Processing”</p>	<p>shall have the meanings given to those terms by the Data Protection Legislation</p>
<p>“Buyer’s Data” “Buyer’s Information”</p>	<p>is any data or information owned or retained to meet departmental business objectives and tasks, including:</p> <p>(a) any data, text, drawings, diagrams, images, or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical, or tangible media, and which are:</p> <ul style="list-style-type: none"> <li>(i) supplied to the Supplier by or on behalf of the Buyer; or</li> <li>(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or</li> </ul> <p>(b) any Personal Data for which the Buyer is the Data Controller;</p>



“Departmental Requirements”	Security	the Buyer’s security policy or any standards, procedures, process, or specification for security that the Supplier is required to deliver.
“Digital Marketplace / G-Cloud”		the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
“End User Devices”		the personal computer or consumer devices that store or process information.
“Good Industry Standard” “Industry Good Standard”		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”		the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: <a href="https://www.gov.uk/government/publications/government-security-classifications">https://www.gov.uk/government/publications/government-security-classifications</a>
“HMG”		Her Majesty’s Government
“ICT”		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)” “IT Health Check (ITHC)” “Penetration Testing”	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 ICT system.
“Need-to-Know”	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.
“NCSC”	the National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is <a href="https://www.ncsc.gov.uk">https://www.ncsc.gov.uk</a>
“OFFICIAL”  “OFFICIAL-SENSITIVE”	the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP).  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” “Role Based Access Control”	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.
“Storage Area Network” “SAN”	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.
“Secure Sanitisation”	the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.

	<p>NCSC Guidance can be found at: <a href="https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media">https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</a></p> <p>The disposal of physical documents and hardcopy materials advice can be found at: <a href="https://www.cpni.gov.uk/secure-destruction-0">https://www.cpni.gov.uk/secure-destruction-0</a></p>
<p>“Security and Information Risk Advisor”</p> <p>“CCP SIRA”</p> <p>“SIRA”</p>	<p>the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: <a href="https://www.ncsc.gov.uk/articles/about-certified-professional-scheme">https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</a></p>
<p>“Senior Information Risk Owner”</p> <p>“SIRO”</p>	<p>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, arm’s length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.</p>
<p>“SPF”</p> <p>“HMG Security Policy Framework”</p>	<p>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. <a href="https://www.gov.uk/government/publications/security-policy-framework">https://www.gov.uk/government/publications/security-policy-framework</a></p>
<p>“Supplier Staff”</p>	<p>all directors, officers, employees, agents, consultants, and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under the Contract.</p>

## Operative Provisions

- 1.1. The Supplier shall be aware of and comply with the relevant [HMG security policy framework](#), [NCSC guidelines](#) and where applicable these Departmental Security Requirements which include but are not constrained to the following paragraphs.
- 1.2. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of [Procurement Policy Note: Updates to the Cyber Essentials Scheme \(PDF\)](#) - [Action Note 09/23](#) dated September 2023, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved and will 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 Buyer.
- 1.3. Where paragraph 1.2 above has not been met, the Supplier 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 Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
- 1.4. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer's Data being handled in the course of providing the Services and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).
- 1.5. Buyer's Data being handled while providing an ICT solution or service must be separated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable

the data to be identified and securely deleted when required in line with paragraph 1.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

- 1.6. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the products or Services, and that store or process Buyer's Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g., door access), CCTV, alarm systems, etc.

- 1.6.1. Where remote working is allowed, the Supplier shall have an appropriate remote working policy in place for any Supplier staff that will have access to the Buyer's data and/or systems.

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

- 1.8. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to:

- 1.8.1. physical security controls;
  - 1.8.2. good industry standard policies and processes;
  - 1.8.3. malware protection;
  - 1.8.4. boundary access controls including firewalls, application gateways, etc;
  - 1.8.5. maintenance and use of fully supported software packages in accordance with vendor recommendations;
  - 1.8.6. use of secure device configuration and builds;
  - 1.8.7. software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

- 1.8.8. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
- 1.8.9. any services provided to the Buyer must capture audit logs for security events in an electronic format at the application, service and system level to meet the Buyer's logging and auditing requirements, plus logs shall be:
  - 1.8.9.1. retained and protected from tampering for a minimum period of six months;
  - 1.8.9.2. made available to the Buyer on request.
- 1.9. The Supplier shall ensure that any Buyer's Data (including email) transmitted over any public network (including the Internet, mobile networks, or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.
- 1.10. The Supplier shall ensure that any Buyer's 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 Buyer except where the Buyer has given its prior written consent to an alternative arrangement.
- 1.11. The Supplier shall ensure that any device which is used to process Buyer's 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>.
- 1.12. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer's 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".

- 1.13. When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer's 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 paragraph 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.

- 1.14. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier's assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier's organisation in line with paragraph 1.15.
- 1.15. In the event of termination, equipment failure or obsolescence, all Buyer's Data and Buyer's Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier 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 Supplier shall protect (and ensure that any sub-contractor protects) the Buyer's Information and Buyer's Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

- 1.16. Access by Supplier Staff to Buyer's 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 Buyer. All Supplier Staff must complete this process before access to Buyer's Data is permitted. [Any Supplier 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].

- 1.17. All Supplier Staff who handle Buyer's Data shall have annual awareness training in protecting information.
- 1.18. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier 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 an 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 must include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 1.19. Any suspected or actual breach of the confidentiality, integrity, or availability of Buyer's Data, including user credentials, used or handled while providing the Services shall be recorded as a Security Incident. This includes any non-compliance with the Departmental Security Requirements and these provisions, or other security standards pertaining to the solution.

Security Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery and followed up in writing. If Security Incident reporting has been delayed by more than 24 hours, the Supplier should provide an explanation about the delay. Regular updates on the Security Incident shall be provided to the Buyer in writing until the incident is resolved.

Security Incidents shall be reported through the Buyer's nominated system or service owner.



Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

- 1.20. The Supplier shall ensure that any Supplier ICT systems and hosting environments that are used to handle, store or process Buyer's Data, including Supplier ICT connected to Supplier ICT systems used to handle, store or process Buyer's 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. On request by the Buyer, the findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required, to be determined by the Buyer upon review of the ITHC findings.
- 1.21. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process, or store Buyer's Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.
- 1.22. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services annually, 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 Services being supplied and the Supplier's, and any sub-contractors', compliance with the paragraphs contained in this Schedule.
- 1.23. The Supplier 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 Buyer through the life of the contract. This will include obtaining any necessary professional security resources required to support the Supplier'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.
- 1.24. Where the Supplier is delivering an ICT solution to the Buyer 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 Buyer's Policy. The Supplier will

provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer's expectation is that the Supplier shall provide written evidence of:

- 1.24.1. implementation of the foundational set of cyber defence safeguards from the Center for Internet Security Critical Security Controls (CIS CSC v8).
- 1.24.2. any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification issued by an organisation accredited by the United Kingdom Accreditation Service.
- 1.24.3. 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.
- 1.24.4. documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Supplier shall provide details of who the awarding body or organisation will be, and date expected.
- 1.24.5. compliance with the principles of Secure by Design as described at [Secure by Design Principles - UK Government Security](#).

Additional information and evidence to that listed above may be required to ensure compliance with DfE security requirements as part of the DfE security assurance process. Where a request for evidence or information is made by the Buyer, the Supplier will acknowledge the request within 5 working days and either provide the information within that timeframe, or, if that is not possible, provide a date when the information will be provided to the Buyer. In any case, the Supplier must respond to information requests from the Buyer needed to support the security assurance process promptly and without undue delay.

- 1.25. The Supplier shall contractually enforce all these Departmental Security Requirements onto any third-party suppliers, sub-contractors or partners who will have access to the Buyer's Data in the course of providing the Services, before access to the data is provided or permitted.

- 1.26. The Supplier shall comply with the [NCSC's social media guidance: how to use social media safely](#) for any web and social media-based communications. In addition, any Communications Plan deliverable must include a risk assessment relating to the use of web and social media channels for the programme, including controls and mitigations to be applied and how the NCSC social media guidance will be complied with. The Supplier shall implement the necessary controls and mitigations within the plan and regularly review and update the risk assessment throughout the contract period. The Buyer shall have the right to review the risks within the plan and approve the controls and mitigations to be implemented, including requiring the Supplier to implement any additional reasonable controls to ensure risks are managed within the Buyer's risk appetite.
- 1.27. Any Supplier ICT system used to handle, store, or process the Buyer's Data, including any Supplier ICT systems connected to systems that handle, store, or process the Buyer's Data, must have in place protective monitoring at a level that is commensurate with the security risks posed to those systems and the data held. The Supplier shall provide evidence to the Buyer upon request of the protective monitoring arrangements in place needed to assess compliance with this requirement.
- 1.28. Where the Supplier is using Artificial Intelligence (AI) and/or Machine Learning (ML) in the delivery of their service to the Buyer, this shall comply with the NCSC's [principles for the security of machine learning](#).

## Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	<b>[insert name of Buyer] ("the Buyer")</b> And <b>[insert name of Supplier] ("the Supplier")</b>	
Contract name:	<b>[insert name of contract to be changed] ("the Contract")</b>	
Contract reference number:	<b>[insert contract reference number]</b>	
Details of Proposed Variation		
Variation initiated by:	<b>[delete]</b> as applicable: Buyer/Supplier]	
Variation number:	<b>[insert variation number]</b>	
Date variation is raised:	<b>[insert date]</b>	
Proposed variation		
Reason for the variation:	<b>[insert reason]</b>	
A Variation Impact Assessment shall be provided within:	<b>[insert number]</b> days	
Impact of Variation		
Likely impact of the proposed variation:	<b>[Supplier to insert]</b> assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> <li><b>[Buyer to insert]</b> original Clauses or Paragraphs to be varied and the changed clause]</li> </ul>	
Financial variation:	Original Contract Value:	£ <b>[insert amount]</b>
	Additional cost due to variation:	£ <b>[insert amount]</b>
	New Contract value:	£ <b>[insert amount]</b>

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address