



Crown Commercial Service

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

Contents

Part A - Order Form.....	2
Order Form Schedule 1 - Services.....	27
Section 1: Project Overview:	27
Section 2: The Services:	27
Section 3: Service Levels	44
Section 4: Supplier resource allocation;.....	53
Section 5: Governance;.....	56
Section 6: Buyers Responsibilities;	62
Annex 1 – Processing Personal Data	66
Annex 2 - Joint Controller Agreement – Not applicable	68
Order Form Schedule 2 - Call-Off Contract Charges	72
Section 1: Resource Charges	72
Section 2 – Managed Service	74
Section 3 – Third Party Pass Through	74
Annex 1 – Third Party Services.....	74
Part B – Terms and Conditions	75
Collaboration Agreement Schedule 1 - List of contracts.....	102
[Collaboration Agreement Schedule 2 - Outline collaboration plan]	103

Part A - Order Form

Digital Marketplace service ID number:	357767035212207
Call-Off Contract reference:	Con_4474
Call-Off Contract title:	Digital Solutions for Test and Trace Service
Call-Off Contract description:	Provide digital solution design, build, and live service to support the Covid-19 National Test service.
Start date:	20 th June 2020
Expiry date:	31 st March 2021
Call-Off Contract value:	The maximum Call-Off Contract value shall be £45 million (forty-five million pounds sterling) excluding VAT (" Maximum Call-Off Contract Value ").
Charging method:	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div>
Purchase order number:	TBA

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

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

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

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

From: the Buyer	NHS Digital Buyer's main address: 1, Trevelyan Square (Head Office), 1 st Floor, Boar Lane, Leeds,
------------------------	---

	LS1 6AE
To: the Supplier	Deloitte LLP +44 (0)20 7936 3000 Supplier's address: Hill House 1 New Street Square LONDON EC4A 3HQ UK Company number: OC 303675
Together: the 'Parties'	

Principle contact details

For the Buyer:	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
For the Supplier:	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

Call-Off Contract term

Start date:	This Call-Off Contract starts on 20 th June 2020 and is valid until 31 st March 2021.
Ending (termination):	<p>The Buyer's rights to End the Contract are as set out in clause 18.</p> <p>The notice period to be provided in accordance with clause 18.6 for the Supplier to End the Call-Off Contract following non-payment of undisputed sums by the Buyer is at least 90 Working Days from the date of written notice for undisputed sums.</p> <p>The parties acknowledge and agree that the provisions set out in the Call-Off terms and conditions relating to Ending the Call-Off Contract shall be the sole options for either party to End the Call-Off Contract and shall supersede and replace any provisions set out in the Supplier Terms relating to termination. The provisions set out in clause 14 of the Supplier Terms shall hereby be disapplied for this Call-Off Contract.</p>
Extension period:	Any extension will be in accordance with the Variation process.

Buyer contractual details

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

G-Cloud Lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud software Lot 3 - Cloud support
G-Cloud Services required:	The Services to be provided by the Supplier under the above Lots are listed in Framework Section 2 and outlined below: <ul style="list-style-type: none">• Cloud Technology Transformation Programme 407950747047842;• Cloud Architecture and Design 994921839625337;• Cloud, Hosting, Infrastructure and Application Planning & Delivery 357767035212207;• Cloud Testing 212391844129173;• Cyber Security and Data Risk 164559172414441;• Data visualisation 602034501977865; and• Salesforce Cloud Solutions 770465150074303.
Additional Services:	N/A
Location:	The Services will be delivered remotely by the Supplier however the Supplier shall comply with reasonable requests by the Buyer to co-locate where practical to facilitate integration of the Services between the Parties.
Quality standards:	The quality standards required for this Call-Off Contract are in accordance with Good Industry Practice.
Technical standards:	The technical standards required for this Call-Off Contract are those applicable to Good Industry Practice. Cyber security standards are defined in Schedule 6 Glossary "Cyber Security Requirements" and Order Form Schedule 1 where appropriate, in line with Good Industry Practice.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as set out in Section 3 of Order Form Schedule 1.
Onboarding:	The Services provided in this Call-Off Contract are already live. The Parties shall establish working practises in accordance with the provisions set out in Order Form Schedule 1 to enable the proper management and transition of the Services from the Supplier to a Replacement Supplier (if applicable) following the End of the Term.
Offboarding:	The Supplier will comply with all reasonable requests from the Buyer to support the exit of the Services including but not limited to the offboarding plan and exit support for this Call-Off Contract as set out in Section 5 (Governance) of Order Form Schedule 1.
Collaboration agreement:	N/A

	<div> <div></div> <div></div> <div></div> </div> <p>Other sub-contractors:</p> <ul style="list-style-type: none"> <div></div> – this subcontractor will not be processing any personal data under the terms of this Call-Off Contract
--	--

Call-Off Contract charges and payment

The Call-Off Contract Charges and payment details are in the table below. See Schedule 2 to this Order Form for a full breakdown.

Payment method:	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>
Payment profile:	<div> <div></div> <div></div> <div></div> </div>
Invoice details:	<p>The Supplier will issue electronic invoices monthly in accordance with the process set out in Section 5 (Governance) of Order Form Schedule 1. The Buyer will pay the Supplier within 30 days of receipt of a valid approved invoice.</p>
Who and where to send invoices to:	<p>Any queries regarding outstanding payments should be directed to NHS Digital's Accounts Payable section by email at Sbs-w.payables@nhs.net.</p> <p>Invoices should clearly quote the purchase order number, be addressed to NHS Digital, T56 Payables A125, Phoenix House, Topcliffe Lane, Wakefield, WF3 1WE and be sent as a PDF attachment by email to the following email address; sbs.invoicing@nhs.net (one invoice per PDF) and emails must not exceed 10Mb and quote, 'T56 Invoice Scanning' in subject line or alternatively invoices can be sent via post to the above address.</p>
Invoice information required – for example purchase order, project reference:	<p>All invoices must include a valid purchase order number.</p> <div> <div></div> <div></div> <div></div> </div>
Invoice frequency:	<div> <div></div> <div></div> <div></div> </div>

Call-Off Contract value:	Unless otherwise agreed by both parties in accordance with the Variation procedure, the maximum Call-Off Contract value shall be £45 million (forty-five million pounds sterling) excluding VAT.
Call-Off Contract charges:	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 15%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 70%;"></div>

Additional Buyer terms

Performance of the service and deliverables:	<p>This Call-Off Contract shall include the scope of services and deliverables as set out in Order Form Schedule 1.</p> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 80%;"></div> <p>All Personal Data processed as part of the Services will remain [REDACTED].</p> <p>The Supplier shall comply with reasonable requests by the Buyer to allow integration of the Services between the Parties.</p>
Guarantee:	Not applicable.
Warranties and representations:	<p>In addition to the incorporated Framework Agreement clause 4.1, the Supplier will comply with the warranties and representations set out in the Buyer specific amendments to/refinements of the Call-Off Contract terms. [REDACTED]</p> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 70%;"></div> <p>The Parties acknowledge and agree that no Deliverables are developed pursuant to the waterfall methodology as referenced in the Supplier Terms.</p>
Supplemental requirements in addition to the Call-Off terms:	<p>In addition:</p> <ol style="list-style-type: none"> 1. The following requirements shall take priority above all terms, conditions and specifications set out in this Call-Off Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that any software licences entered into from the date of this Call-Off Contract used to provide the Services meet and conform with the following requirements: <ol style="list-style-type: none"> 1.1 <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 95%;"></div> 1.2 <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div>

	<p>1.3 [REDACTED]</p> <p>1.4 [REDACTED]</p> <p>1.5 [REDACTED]</p> <p>For the avoidance of doubt, the Supplier does not provide the above assurances for the software in use for the existing live solution in place as at the date of this Call-Off Contract.</p> <p>2 In addition to paragraph 1 above, the following requirement shall take priority above all terms, conditions and specifications set out in this Call-Off Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that any software licences including those entered into prior to the Start Date of this Call Off Contract used to provide the Services meet and conform with the following requirement:</p> <p>2.1 The Supplier shall ensure that the Buyer shall be entitled [REDACTED]</p> <p>3. By signature of this Call-Off Contract, the Buyer acknowledges and agrees that the Supplier's reporting of the quality and performance of the Services and Deliverables provided by the Supplier between 20th June 2020 and 30th November 2020 (inclusive) has been agreed by the Parties and the Buyer will not withhold any Charges for this period.</p>		
Alternative clauses:	These Alternative Clauses, which have been selected from Schedule 4, will apply: N/A.		
Buyer specific amendments to/refinements of the Call-Off Contract terms:	<p>For the purposes of incorporation of Schedule 6 - Glossary and interpretations of the Call-Off terms, the following definitions shall be added (and where such terms are already defined, such definitions shall be replaced with the corresponding definitions below):</p> <table border="1"> <tr> <td>Central Government Body</td><td> <p>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <p>a) Government Department;</p> </td></tr> </table>	Central Government Body	<p>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <p>a) Government Department;</p>
Central Government Body	<p>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <p>a) Government Department;</p>		

		<p>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);</p> <p>c) Non-Ministerial Department; and</p> <p>d) Executive Agency;</p>
	Comparable Supply	the supply of deliverables to another buyer of the Supplier that are the same or similar to the Deliverables;
	Contracts Finder	the Government's publishing portal for public sector procurement opportunities;
	Corporate Security	includes but not limited to the relevant Party's Employee or third party identity verification and vetting, travel risk management, event security, health and safety, Control of Substances Hazardous to Health, intelligence gathering and briefing on risks and threats to corporate bodies;
	CSR Laws	means Laws relating to corporate social responsibility issues (e.g. anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity), including but not limited to the Modern Slavery Act 2015, the Public Services (Social Value) Act 2012, the Public Contracts Regulations 2015 and Article 6 of the Energy Efficiency Directive 2012/27/EU, from time to time in force;
	CSR Policies	means the Buyer's policies, including, without limitation, anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity, and any similar policy notified to the Supplier by the Buyer from time to time, and " CSR Policy " shall mean any one of them;
	Cyber Security Requirements	<p>means:</p> <p>a) compliance with the DSP Toolkit or any replacement of the same;</p> <p>b) the selection and application of selected controls from the NIST cyber security framework v1.1, and any other compulsory and/or other cyber security requirements relating to the Services notified to the Supplier by the Buyer from time to time; and</p> <p>c) at a minimum, the application and demonstration by the Supplier and any Subcontractors of Good Industry Practice with respect to information security and cyber security;</p>
	Data Guidance	means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding

			information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to the Subprocessor by the Processor. This includes but is not limited to guidance issued by NHS Digital, the National Data Guardian for Health & Care, the Department of Health, the Health Research Authority, Public Health England, NHS England and the European Data Protection Board;
		Deliverable(s)	means the Services (including the G-Cloud Services), the Solution, products, licences and other items that the Buyer contracts the Supplier to provide under this Call-Off Contract;
		DSP Toolkit	means the data security and protection toolkit, an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards and supports key requirements of the GDPR, which can be accessed from https://www.dsptoolkit.nhs.uk/ , as may be amended or replaced by the Buyer or the Department of Health and Social Care from time to time;
		Force Majeure	<p>A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party; • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; • acts of government, local government or Regulatory Bodies; • fire, flood or disaster and any failure or shortage of power or fuel; and • industrial dispute affecting a third party for which a substitute third party isn't reasonably available. <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Suppliers (or a Subcontractor's) supply chain; • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure; • the event was foreseeable by the Party seeking to rely on Force Majeure at the time

			<p>this Call-Off Contract was entered into;</p> <ul style="list-style-type: none"> • non availability of Supplier Staff and any disruption to the Supplier's supply chain and / or relevant third party contracts related to the provision of the Services caused by the Covid-19 Pandemic; and • 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.
		G-Cloud Services	for the purpose of this Call-Off Contract, means the Services and Deliverables ordered by the Buyer as set out in the Order Form;
		General Change in Law	means a change in Law which comes into force after the Start Date, where the change is of a general legislative nature and/or affects or relates to a Comparable Supply, and includes Laws arising out of or in connection with the United Kingdom's withdrawal from the European Union which substantially amend, replace or supersede any existing Law;
		Law	means (from time to time in force) any applicable law, any applicable Act of Parliament, statute, by law, regulation, order, regulatory policy (including any requirement or notice of any regulatory body), guidance or industry code of practice, rule of court or directives or requirements of any Regulatory Body, delegated or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, or enforceable community right within the meaning of Section 2 of the European Communities Act 1972, and any amended or new laws arising out of or in connection with the United Kingdom's withdrawal from the European Union (that is, ceases to be an EU Member State);
		Medical Device	means any Deliverable that falls under the definition of a medical device in accordance with guidance published by the Medicines and Healthcare Products Regulatory Agency;
		Physical Security	includes but not limited to the relevant Party controlling physical access to facilities and sites, implementing or reviewing physical barriers for facilities and sites, creating or maintaining physical integrity of facilities and sites, reducing or preventing harm to employees, third parties or the public from internal or external threats at a facility or site, intelligence gathering and briefing on risks and threats to sites and facilities;

	Processor Personnel	means any and all persons employed or engaged from time to time in the provision of services and/or the Processing of Personal Data whether employees, workers, consultants or agents of the Subprocessor or any subcontractor or agent of the Subprocessor;
	Project Specific IPRs	mean 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 and related predecessor contracts with the Department for Health and Social Care including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs;
	SME	means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
	Solution	means the Supplier's solution as further detailed in Section 2 to Order Form Schedule 1;
	Regulatory or Supervisory Body	means any statutory or other body having authority to issue guidance, standards or recommendations with which the Processor Personnel must comply or to which they must have regard including: <ul style="list-style-type: none"> a) CQC; b) NHS Improvement; c) NHS England; d) The Department of Health and Social Care; e) The National Institute for Health and Care Excellence; f) Healthwatch England and Local Healthwatch; g) Public Health England; h) The General Pharmaceutical Council; i) The Healthcare Safety Investigation Branch; j) Information Commissioner's Office; and k) European Data Protection Board;
	Subprocessor	means the Supplier, or any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract;
	Supplier Software	software which is proprietary to the Supplier and which is or will be used by the Supplier for the purposes of providing the Deliverables;

[illegible]

1) A new paragraph 1.4A shall be added to this Order Form as follows:

2) [REDACTED]

	<div style="text-align: right; margin-bottom: 10px;"> <div style="background-color: black; width: 300px; height: 15px; margin-bottom: 5px;"></div> b) <div style="background-color: black; width: 300px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 200px; height: 15px; display: inline-block;"></div> </div> <p>3) Clauses 12.1 and 12.3 of the Call-Off terms and conditions shall be deleted in their entirety and replaced with the following new clauses 12.1 and 12.3.</p> <p>12.1 The Supplier must:</p> <ul style="list-style-type: none"> • comply with the Buyer's written instructions and this Call-Off Contract when Processing any Buyer Data, including but not limited to Buyer Personal Data; • only Process the Buyer Data, including but not limited to Buyer Personal Data as necessary for the provision of the Services or as required by Law or any Regulatory Body; and • take reasonable steps to ensure that any Supplier Staff who have access to any Buyer Data, including but not limited to Buyer Personal Data act in compliance with Supplier's security processes. <p>12.3 The Supplier must get prior written consent from the Buyer to transfer any Buyer Data, including but not limited to Buyer Personal Data to any other person for the provision of the Services. For transfers of Buyer Data that represent the routine operational function of the Service, these transfers may be authorised by the Buyer in writing as a blanket authorisation for this scoped operational function only. A register of routine transfers can be created and this can be approved in writing as a single occurrence by the Buyer. Further approval will only then be required for transfers that are outside of the scope of this approval. The Buyer can cease and remove this authorisation at any time.</p> <p>4) New clauses 12.4 to 12.8 shall be added to the Call-Off terms and conditions as follows:</p> <p>12.4 The Subprocessor shall not respond substantively to the communications listed at paragraph 6 of Schedule 4 to the Framework Agreement save that it may respond to a Regulatory or Supervisory Body following prior consultation with the Processor.</p> <p>12.5 Without prejudice to paragraph 6 of Schedule 4 to the Framework Agreement, upon the occurrence of a Data Loss Event the Subprocessor shall:</p> <p style="margin-left: 20px;">12.5.1 <div style="background-color: black; width: 500px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 150px; height: 15px; display: inline-block;"></div></p> <div style="margin-left: 100px; margin-top: 10px;"> <div style="background-color: black; width: 550px; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 500px; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 80px; height: 15px; display: inline-block;"></div> </div> <div style="margin-left: 100px; margin-top: 10px;"> <div style="background-color: black; width: 550px; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 500px; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 250px; height: 15px; display: inline-block;"></div> </div> <p style="margin-left: 20px;">12.6 <div style="background-color: black; width: 550px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 550px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 550px; height: 15px; display: inline-block;"></div> <div style="background-color: black; width: 550px; height: 15px; display: inline-block;"></div></p>
--	--

		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>12.7 The Subprocessor shall, in connection with the Personal Data Processed under this Call-Off Contract, maintain complete and accurate records and information to demonstrate its compliance with the Data Guidance.</p> <p>12.8 Neither Party shall do nor omit to do anything that will put the other Party in breach of the Data Protection Legislation.</p> <p>5) A new clause 17A shall be added to the Call-Off terms and conditions as follows:</p> <p>The Supplier warrants and represents that it has all consents, registrations, approvals, licences and permissions relating to Medical Devices as recommended or stipulated by any materials published by the Medicines and Healthcare Products Regulatory Agency.</p> <p>6) Clauses 18.2 and 18.3 of the Call-Off terms and conditions shall be deleted in their entirety and replaced with the following new clauses 18.2 and 18.3:</p> <p>18.2 The Parties agree that the:</p> <ul style="list-style-type: none"> • Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of Cloud Service being provided; and • [REDACTED] <p>18.3 [REDACTED]</p> <p>7) Clause 23.1 of the Call-Off terms and conditions shall be deleted in its entirety and replaced with the following clause 23.1 and 23.2:</p> <p>23.1 If a Force Majeure event prevents either Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the Buyer may End this Call-Off Contract with immediate effect by written notice.</p> <p>23.2 If a Force Majeure event prevents the Supplier from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the Supplier may End this Call-Off Contract by providing the Buyer with a minimum of 90 Working Days written notice from the end of the time period set out in the Order Form.</p> <p>8) The following wording shall be deleted from clause 32.1 of the Call-Off terms and are hereby disapplied:</p>
--	--	---

	<p><i>"if it isn't a material change to the Framework Agreement/ or this Call-Off Contract".</i></p> <p>9) A new clause 32.4 shall be added to the Call-Off terms and conditions and shall take precedence over clause 8.11 of the Framework Agreement for the sole purpose of interpretation of this Call-Off Contract in relation to General Changes of Law:</p> <p>32.4 Any required changes to the Services or this Call-Off Contract after the Start Date arising out of or in connection with the United Kingdom's withdrawal from the European Union (that is, ceases to be an EU Member State) shall be addressed as a General Change in Law, which means the Supplier shall not be entitled to reduce the functionality or performance of the Services or increase the Charges.</p> <p>10) New clauses 4A and 4B shall be added to the Call-Off terms and conditions as follows:</p> <p>4A IR35</p> <p>4A.1 This Call-Off Contract constitutes a contract for the provision of goods and/or services. Where the Supplier (or its Subcontractors) have included one or more people that are non-permanent members of staff that are not on the Supplier's (or its Subcontractors) payroll ("Contractor(s)") to fulfil its service obligations under this Call-Off Contract, [REDACTED]</p> <ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED] <p>4A.2 [REDACTED]</p> <p>4A.3 The Supplier warrants that it is not, nor will it prior to the cessation of this Call-Off Contract, become a managed service company, within the meaning of section 61B of the Income Tax (Earnings and Pensions) Act 2003.</p> <p>4A.4 The Supplier shall monitor the provision of the services and notify the Buyer where it considers that the activity of the Buyer may impact the Suppliers' (or its Subcontractors) IR35 Assessment in relation to the Contractors.</p> <p>4B Security of Supplier Staff</p> <p>4B.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel</p>
--	---

	<p>Security Standard (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as may be amended or replaced by the Government from time to time.</p>
4B.2	The Supplier shall agree on a case by case basis which Supplier Staff roles which require specific government National Security Vetting clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Buyer Data. The Supplier shall provide and maintain a breakdown of the security clearance held for each Supplier Staff role and shall work with the Buyer to propose any necessary amendments to these in order to provide the Services.
4B.3	The Supplier shall prevent Supplier Staff who have not yet received or are unable to obtain the security clearances required by this clause from accessing systems which store, process, or are used to manage Buyer Data, or from accessing Buyer premises, except where agreed with the Buyer in writing.
4B.4	All Supplier Staff that have the ability to access Buyer Data or systems holding Buyer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually, and the Supplier must be able to demonstrate the completion of the training for all in scope staff.
4B.5	Where Supplier Staff are granted the ability to access Buyer Data or systems holding Buyer Data, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need such access but remain employed by the Supplier's organisation, their access rights shall be revoked by the close of business on the following Working Day. When staff no longer need such access and they leave the Supplier's organisation, their access rights shall be revoked by the close of business on the same Working Day.
11)	A new clause 7.2A shall be added to the Call-Off terms and conditions as follows:
7.2A	Electronic Invoicing
7.2A.1	The Buyer shall accept and process for payment an electronic invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.
7.2A.2	For the purposes of clause 7.2A.1, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.
12)	A new clause 16.8 shall be added as follows:
16.8	The Supplier warrants and represents that it has complied with and throughout the Call-Off Contract Term will continue to comply with the Cyber Security Requirements.
13)	Clause 27 of the Call-Off terms and conditions shall be deleted in its entirety and replaced with the following:
27	Third Party Rights
	27.1 Subject to clause 27.2, a person who is not Party to this Call-Off Contract has no right to enforce any term of it under the Contracts (Rights

of Third Parties) Act 1999.

27.2 The Department for Health and Social Care's arm's length bodies, excluding NHS Digital, (being: NHS England, NHS Improvement, Care Quality Commission, National Institute for Health and Care Excellence, Public Health England, Health Education England, Health Research Authority, NHS Blood and Transplant, Medicines and Healthcare Products Regulatory Agency, NHS Business Services Authority, NHS Resolution, Human Fertilisation and Embryology Authority, Human Tissue Authority and NHS Counter Fraud Authority) and any successors or replacements thereof [REDACTED]

[REDACTED]

[REDACTED]

- 14) For the purposes of incorporating clause 8.8 of the Framework Agreement into this Call-Off Contract, the following wording shall be added after "as expressly set out in this Framework Agreement":

[REDACTED]

- 15) A new clause 28A shall be added to the Call-Off terms and conditions as follows:

28A Corporate Social Responsibility Conduct and Compliance


28A.1 The Buyer applies corporate and social responsibility values to its business operations and activities which are consistent with the Government's corporate social responsibility policies, including, without limitation, those policies relating to anti-bribery and corruption, health and safety, the environment and sustainable development, equality and diversity.

28A.2 The Supplier represents and warrants that it:

28A.2.1 complies with all CSR Laws;

	<p>28A.2.2 requires its Subcontractors and any person under its control, to comply with all CSR Laws; and</p> <p>28A.2.3 has adopted a written corporate and social responsibility policy that sets out its values for relevant activity and behaviour (including, without limitation, addressing the impact on employees, clients, stakeholders, communities and the environment by the Supplier's business activities).</p> <p>28A.3 The Supplier shall notify the Buyer in the event that its corporate and social responsibility policies conflict with, or do not cover the same subject matter in an equivalent level of detail as is in, the CSR Policies.</p> <p>16) A new clause 28B shall be added to the Call-Off terms and conditions as follows:</p> <p>28B Modern Slavery</p> <p>28B.1 The Supplier represents and warrants that at the Start Date neither the Supplier, nor any of its officers and employees:</p> <p>28B.1.1 have been convicted of any offence involving slavery and human trafficking; and</p> <p>28B.1.2 having made reasonable enquiries, so far as it is aware, have been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking.</p> <p>28B.2 The Supplier shall implement due diligence procedures for its Subcontractors and other participants in its supply chains to ensure that there is no slavery or human trafficking in its supply chains.</p> <p>28B.3 The Supplier shall prepare and deliver to the Buyer each year, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.</p> <p>17) A new clause 33.2 shall be added to the Call-Off terms and conditions as follows:</p> <p>33.2 The Supplier shall, participate and provide full co-operation for the completion of any Data Protection Impact Assessments conducted by the Buyer relating to the Services and the Deliverables, such participation and co-operation shall include updating the Data Protection Impact Assessment upon each release and following any Variation.</p> <p>18) A new clause 34 shall be added to the Call-Off terms and conditions as follows:</p> <p>34 Assignment and Novation</p> <p>The Buyer may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Call-Off Contract and/or any associated licences to the Department of Health and Social Care, NHS England and / or any Central Government Body and the Supplier shall, at the Buyer's request, enter into an agreement in such form as the Buyer shall reasonably specify in order to enable the Buyer</p>
--	--

	<p>to exercise its rights pursuant to this clause 34 (Assignment and Novation).</p> <p>19) A new clause 35 shall be added to the Call-Off terms and conditions as follows:</p> <p>35 Subcontracts</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>20) A new clause 36 shall be added to the Call-Off terms and conditions as follows:</p> <p>36. Improving visibility of subcontract opportunities available to SMEs and VCSEs in the supply chain</p> <p>36.1 The Supplier shall:</p> <p>36.1.1 subject to clause 36.1.3, advertise on Contracts Finder all subcontract opportunities arising from or in connection with the provision of the Services above a minimum threshold of £25,000 that arise during the Term;</p> <p>36.1.2 within 90 days of awarding a Subcontract to a Subcontractor, update the notice on Contracts Finder with details of the successful Subcontractor;</p> <p>36.1.3 monitor the number, type and value of the Subcontract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Term;</p> <p>36.1.4 provide reports on the information at clause 36.1.3 to the Buyer in the format and frequency as reasonably specified by the Buyer; and</p> <p>36.1.5 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.</p> <p>36.2. Each advert referred to at clause 36.1.1 above shall provide a full and detailed description of the subcontract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.</p> <p>36.3. The obligation at clause 36.1.1 shall only apply in respect of subcontract opportunities arising after the contract award date.</p> <p>36.4. Notwithstanding clause 36.1, the Buyer may by giving its prior written approval, agree that a subcontract opportunity is not required to be advertised on Contracts Finder.</p> <p>21) A new clause 37 shall be added to the Call-Off terms and conditions as follows:</p> <p>37. Management Charges and Information</p> <p>37.1. In addition to any other management information requirements set out in</p>
--	---

	<p>this Call-Off Contract, the Supplier agrees and acknowledges that it shall, provide timely, accurate and complete SME Management Information (MI) Reports to the Buyer which incorporate the data described in the MI Reporting template which is:</p> <p>37.1.1 the total contract revenue received directly on a specific contract;</p> <p>37.1.2 the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and</p> <p>37.1.3 the total value of subcontracted revenues to SMEs and VCSEs.</p> <p>37.2. The SME Management Information Reports shall be provided in the correct format as required by the MI Reporting Template and any guidance issued by the Buyer from time to time. The Supplier shall use the initial MI Reporting Template which is set out in Schedule 1 of the Framework Agreement and which may be changed from time to time (including the data required and/or format) by the Buyer by issuing a replacement version. The Buyer shall give at least thirty (30) days' notice in writing of any such change and shall specify the date from which it must be used.</p> <p>37.3. The Supplier further agrees and acknowledges that it may not make any amendment to the current MI Reporting Template without the prior written approval of the Buyer.</p> <p>22) A new clause 38 shall be added to the Call-Off terms and conditions as follows:</p> <p>38 Execution and Counterparts</p> <p>38.1 This Call-Off Contract may be executed in any number of counterparts (including by electronic transmission), each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument.</p> <p>38.2 Execution of this Call-Off Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Call-Off Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Call-Off Contract as if signed by each Party's manuscript signature. In such situation, this Call-Off Contract shall be formed on the date on which both Parties have electronically signed the Call-Off Contract as recorded in the Buyer's electronic contract management system.</p> <p>23) Schedule 4 - Processing Data (Framework Agreement)</p> <p>23.1) </p> <p>23.2) For the purposes of incorporating Schedule 4 of the Framework Agreement into this Call-Off Contract, paragraph 5(d) shall be deleted in its entirety and replaced with the following:</p>
--	---

(d) [REDACTED]
[REDACTED]
[REDACTED]

(i) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(ii) [REDACTED]
[REDACTED]

(iii) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(iv) [REDACTED]
[REDACTED]
[REDACTED]

23.3) For the purposes of incorporating Schedule 4 of the Framework Agreement into this Call-Off Contract, a new paragraph 5A shall be added to Schedule 4 of the Framework Agreement as follows:

5A.1 The Supplier acknowledges that that, following the end of the transition period under the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (The EU-UK Withdrawal Agreement) the UK will be treated as a third country for the purposes of the GDPR. Therefore, any transfers of Personal Data between the Supplier's EU processing operations and the Buyer may be restricted.

5A. [REDACTED]
[REDACTED]
[REDACTED]

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

23.4) The reference to paragraph 16 in paragraph 28 of Schedule 4 of the Framework Agreement shall be deleted and replaced with a reference to paragraph 17.

24) An extra row shall be added at the end of the table at Annex 1 of Schedule 7 (GDPR Information) as follows:

Jurisdiction of processing	[REDACTED]
-----------------------------------	------------

Public Services Network (PSN):	Not applicable
Personal Data and Subjects:	<p>Confirm whether either Annex 1 or Annex 2 of Schedule 7 is being used: Annex 1 as further detailed in Annex 1 to Order Form Schedule 1</p> <p>The parties agree that the provisions in paragraph 17.4 of the Supplier Terms shall be disapplied.</p>

1. Formation of contract

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



deloitte-g-cloud-11
-standard-terms-anc

2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.
- (B) The Buyer provided an Order Form for Services to the Supplier.
- (C) The individuals set out below shall execute this Call-Off Contract, on behalf of the Buyer and the Supplier, either using a manuscript signature or an electronic signature. A manuscript signature shall be placed in the execution block below, an electronic signature shall be evidenced in an execution block to be attached as the final page of this Call-Off Contract:

Signed:	Supplier	Buyer
Name of individual signing:	██████████	██████
Title:	██████	██████████████████
Email:	██████████████████	██████████
Signature (only applicable for manuscript signature):		
Date (only applicable for manuscript signature):		

Order Form Schedule 1 - Services

Section 1: Project Overview:

The Buyer's objective is to deliver a nationwide integrated coronavirus Test and Trace service, which forms a central part of the government's coronavirus recovery strategy. NHS Test and Trace brings together four tools to control the virus:

- Test: increasing availability and speed of testing will underpin NHS Test and Trace;
- Trace: when someone tests positive for coronavirus the NHS Test and Trace service will identify any close recent contacts and alert those who need to self-isolate;
- Contain: a national Joint Biosecurity Centre will work with local authorities and public health teams in Public Health England (PHE), including local Directors of Public Health, to identify localised outbreaks and support effective local responses, including plans to quickly deploy testing facilities to particular locations; and
- Enable: government to learn more about the virus, including as the science develops, to explore how the Parties could go further in easing infection control measures.

Coronavirus tests in the UK are carried out through a number of different routes:

Pillar 1: swab testing in Public Health England (PHE) labs and NHS hospitals for those with a clinical need, and health and care workers;

Pillar 2: swab testing for the wider population, as set out in government guidance;

Pillar 3: serology testing to show if people have antibodies from having had COVID-19; and

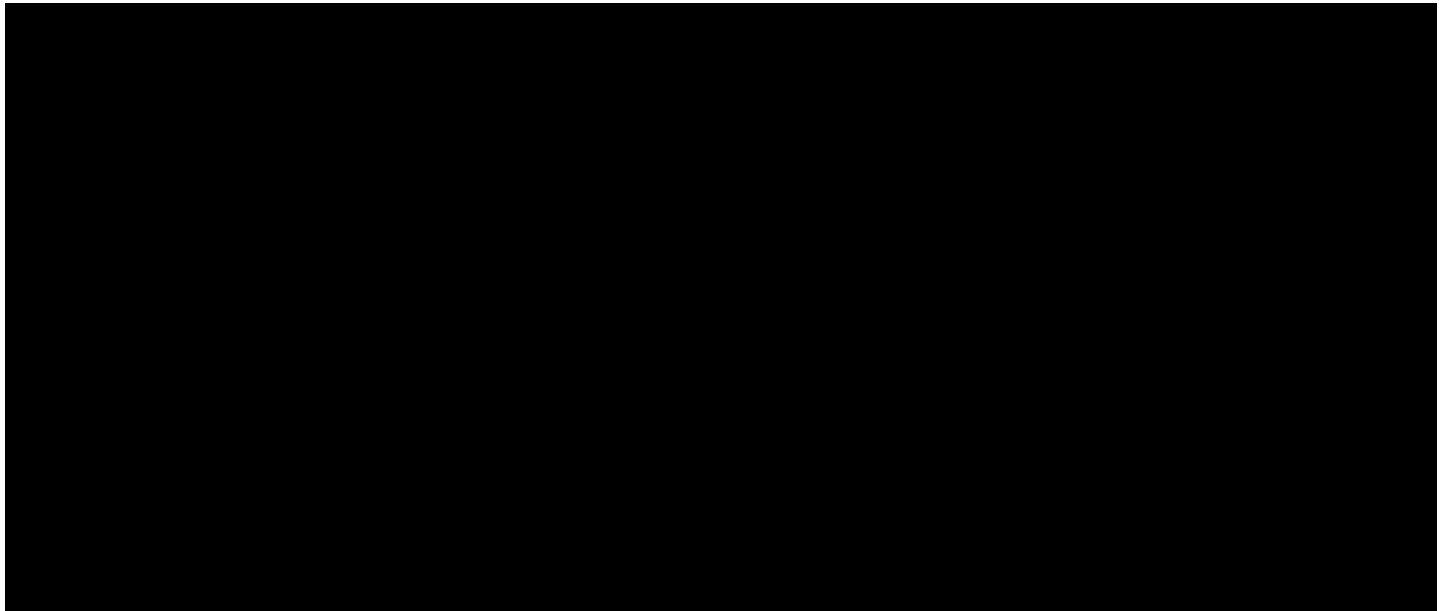
Pillar 4: blood and swab testing for national surveillance supported by PHE, the Office for National Statistics (ONS), and research, academic, and scientific partners to learn more about the prevalence and spread of the virus and for other testing research purposes, such as the accuracy and ease of use of home testing.

Section 2: The Services:

Section 2.1 Overview of the Services and Solution:

The Supplier shall provide the Services in accordance with the terms of this Call-Off Contract. The Services shall be delivered in relation to the national coronavirus testing regime for Pillar 2 and 3. Pillar 4 is currently out of scope of the Service, but may be covering in future work as instructed by the Buyer.

The diagrams below summarises the key components in the testing digital service, highlighting those operated by the Supplier (Deloitte) as part of the Services (the '**Solution**').



(note this diagram does not attempt to show all integration points or users)



Details of Supplier provided Solution as set out above:

Component	Purpose	
Core Digital Platform for Testing	Manages the user journey for the subject from referral through to test sample submission. Master data source for testing lifecycles.	serverless platform using capabilities throughout (, etc.)
Employer Referral Portal	Enables employers to refer bulk lists of staff for testing.	Outsystems portal with UI Path processing logic
Satellite Manager Ordering Portal	Enables bulk test kit orders (e.g. for care homes).	
Mobile Apps	Provides tools for field force to register samples, look up subjects, validate sample age and more.	Native apps deployed onto dedicated locked-down
MI Platform (until 31 st August 2020 only)	Enables business users to query and analyse operational and strategic data about service and performance. The parties acknowledge and agree that this platform will be split, moving the staging activities into NHS infrastructure and tableau visualisation into DHSC control.	data platform. On top of warehouse and based data lake, all hosted on

The Services provided by the Supplier are summarised and explained in more detail in the sections that follow.

- Service 1.** Cloud Technology Transformation Programme - shapes, integrates, and manages the other six services listed below. These services provide oversight for the teams that provide the services outlined below. This service also coordinates with the Buyer and other parties within and outside the Test and Trace programme.
- Service 2.** Cloud services that support the Buyer's Coronavirus (COVID-19) subject test service Services that deliver the Solution.
- Service 2.1.** Cloud Architecture and Design – supports the Buyer in shaping its backlog and roadmap, and translating the backlog into functional and User Experience (UX) designs (including usability research and copywriting), and architecture and technology design so that the Supplier is ready to build into the Solution (executed in Service 2.2).
- Service 2.2.** Cloud, Hosting, Infrastructure and Application Planning & Delivery – builds the Solution functional, UX and technical designs developed in Service 2.1, through provision of IT infrastructure, developing bespoke software and package configuration. This includes technical release management, service delivery management, service analysts and a service desk to run the live service.
- Service 2.3.** Cloud Testing – functional and non-functional testing of the releases developed in Service 2.2. This includes automation testing and security, and performance testing of the Solution including digital application and mobile applications.
- Service 3.** Cyber Security Services – within the scope of Services 2,3,4,5 design, build and operate the Solution with the cyber and data privacy controls necessary to achieve the Buyer's defined business objectives and defined cyber risk tolerances. This includes consideration of the information security governance and data risk.
- Service 4.** Data visualisation (MI Platform) – data engineering and management information design, build and live operation of the Management Information (MI) Platform. This Service will only be provided under this Call Off Contract until the 31st August 2020.
- Service 5.** Salesforce Cloud Services (Satellite Manager Ordering Portal) – design and build and live operation of a Salesforce Cloud Service, the part of the Solution which will allow bulk ordering of test kits, initially for care homes but extendable to other organisations.

Together these Services provide the Solution as captured in Section 2.1 of this Order Form Schedule 1, and are delivered via the resource structures as set out in Section 4 to this Order Form Schedule 1.

Section 2.2 Detailed Description of Services

Service 1: Cloud Technology Transformation Programme

This service shapes, integrates, and manages all of the Services. This service provides oversight for the teams that provide the Services 2 to 5 outlined below. Included in this Service 1, the Supplier shall:

- Manage and integrate the teams providing Services 2 to 5 to deliver an integrated service to the Buyer;
- Engage with the Buyer's business and IT teams to shape and contribute to the Buyer's roadmap;
- Engage, participate and collaborate with the Buyer's Governance and Assurance forums;

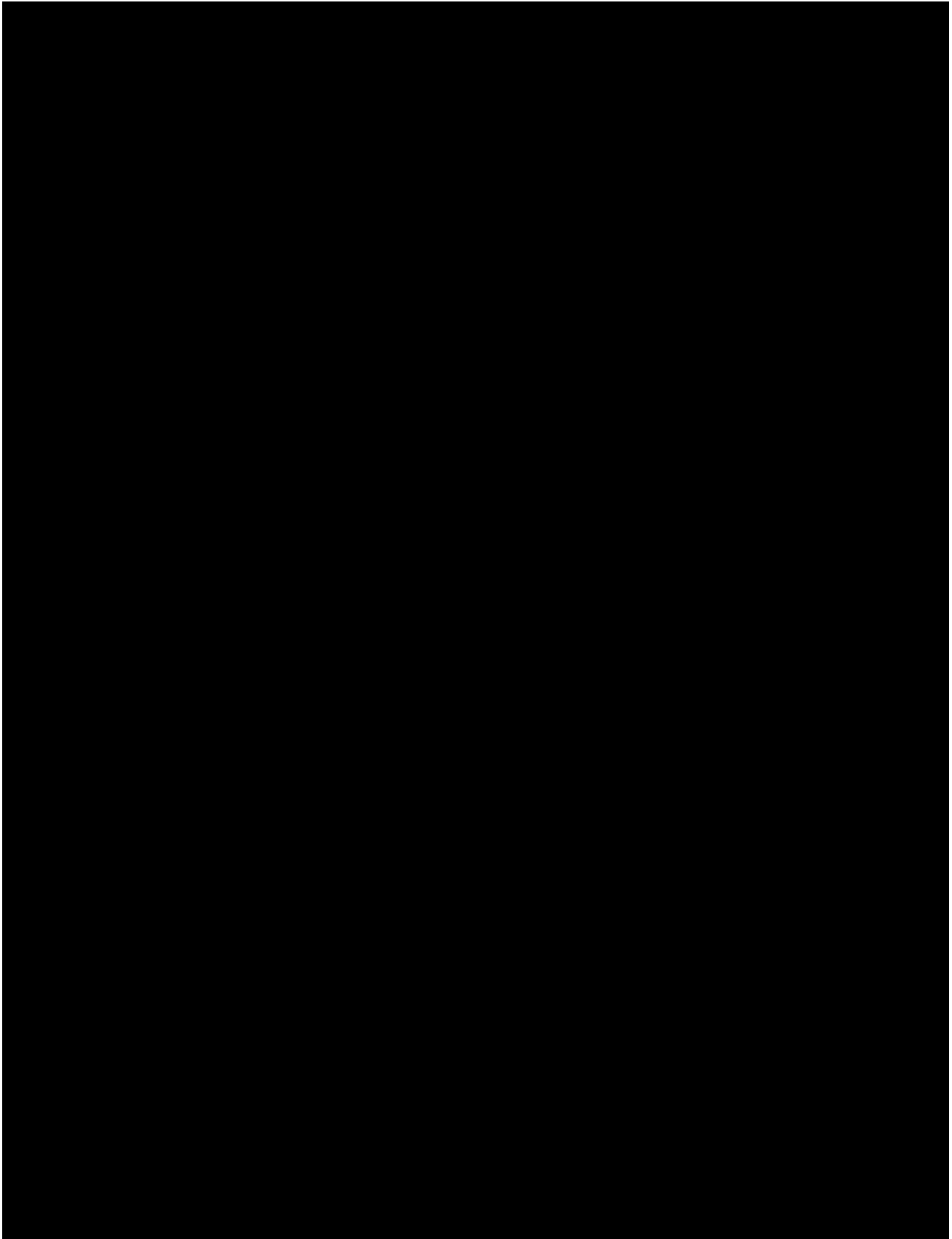
- Plan, track and manage the delivery and technical releases of the Supplier's Solution;
- Engage with third party suppliers required to deliver the Supplier's scope; and
- Provide PMO services for the Supplier's team and support the Central Test and Trace (Pillar 2) PMO with for example: weekly and ad-hoc reporting on progress, RAID log, and budget analysis.

The Supplier will participate and provide any information requested by the Buyer to support the Buyer's governance and assurance.

Service 2: Cloud services that support the Buyer's Coronavirus (COVID-19) subject test service

The following Services 2.1, 2.2, 2.3 together support the Supplier's provided Solution.

Changes to the Solution will be captured by the Buyer and agreed through the governance process set out in Section 5 to this Order Form Schedule 1 .



[REDACTED]

[REDACTED]

Overview of Mobile Apps

The mobile apps comprise of a suite of apps provided for operatives in the field. The current settings for these users are (a) at Regional, Local or Mobile test sites and (b) in labs, however provision is made for other settings to be introduced as required.

There are currently six apps available for use by site & lab operatives. The mobile apps delivered as part of the Solution are as follows:

1. **Register App:**

Encapsulates the “registration lite” journey to enable site staff to register Subjects on site and associate a Sample ID with the Subject.

2. **Inventory App:**

Encapsulates the “Inventory management [REDACTED] website” to enable site staff to perform inventory management tasks.

3. **Security App:**

Enables security staff on site to look up a Subject's appointment details. This is completed by searching for the Subject's car registration number or date of birth, or by scanning a Subject ID QR Code to retrieve and validate a Subject's appointment.

4. **Check-in App:**

Enables Check-in staff on site to associate a Sample ID with a Subject ID. This is done by scanning or manually entering both IDs.

5. **Dispatch App:**

Enables staff to count and reconcile the number and IDs of Samples in a [REDACTED] container and record the date and time the container is handed to the courier service for delivery, and which lab it will be delivered to.

6. **Validate App:**

Enables staff at labs to confirm the arrival of the [REDACTED] containers from testing sites, reconcile the number of samples in each container and verify the viability of the sample with regards to the time left on the lifespan of the vial and prioritise the testing of the samples in relation to samples in other containers/deliveries.

Service 2.1: Cloud Architecture and Design

Working with the governance process set out in Section 5 to this Order Form Schedule 1 this service supports shaping of the Solution (covering backlog and future roadmap), and translates the backlog into functional and User Experience (UX) designs (this includes usability research and copywriting), and architecture and technology design ready to change the Solution (executed in Service 2.2).

As part of this service the Supplier shall provide the following activities:

- Participate in the creation and prioritisation of the Buyer's product roadmap including functional and architectural impact assessments of new features and relevant user research;
- Collaborate on and develop with the Buyer the end to end journey for subject and test registration across testing channels;

- Collaborate on and develop with the Buyer the subject/customer journey for programme [REDACTED] device users at test sites (RTS, LTS, MTU) and in labs to support the operational efficiency of the programme within the bounds of the Solution;
- High level functional scope, UX and copy design of new journeys and/or enhanced user journeys to enable the prioritisation, design and build activities of features in the product roadmap;
- Architecture and technical design for example microservice and no-SQL based solution architecture, design of new or changes to Application Programming Interfaces (APIs), data export process to [REDACTED], changes to support the Management Information (MI) & Analytics solution, SMS and email flow to the GOV-Notify service, authentication solution based on [REDACTED] for authenticated web journey and mobile applications; and
- Functional design, feature and user story elaboration to support development (executed in Service 2.2).

A number of third-party applications and toolsets (as set out in Annex 1 of Order Form Schedule 2) are required by the Supplier to deliver the functional releases of software as defined above. The Supplier will configure, maintain and manage access to these applications and toolsets in order to complete the activities and deliverables specified under this Call Off Contract.

Services 2.2: Cloud, Hosting, Infrastructure and Application Planning & Delivery

This service delivers the functional, UX and technical designs of the Solution defined in Service 2.1 and within the scope of this Call-Off Contract. It includes provisioning IT infrastructure (using [REDACTED]), developing bespoke software and package configuration, and release management and running the live service.

The following activities shall be provided by the Supplier as part of the Solution in compliance with the agreed assurance activities:

- Implement cloud custom code, platform configuration and mobile app ([REDACTED]) applications and systems;
- Development of fixes for defects identified by the Cloud Testing team (Service 2.3);
- Design, build and maintain the non-production and production environments;
- Implement new or changed [REDACTED] services and design, build and deploy infrastructure components;
- Release management and documentation of release artefacts to deploy code and releases to the non-production and production environments, and participate and collaborate with the Buyer's assurance processes (e.g. CAB);
- Provide live support as set out in Section 3 of this Order Form Schedule 1;
- Propose and initiate the first steps on creating a shared toolset and shared platform that will allow a multi supplier ecosystem to deliver code; and
- Support transition of hosting services to the Buyer or Buyer nominated party (if requested).

Service 2.3: Cloud Testing

This Service provides test management, preparation, execution, automation scripting, defect management and completion reporting for the Solution in accordance with the output of Service 2.2. This

Service, the outcome of the tests and the information provided by the Supplier informs the Buyer's decision making on whether the Supplier's releases to the Solution are ready for introduction into live operation for use by the Buyer's intended audience.

The service includes:

- Test Approaches – a high-level test approach outlining the key test activities and scope of test for a release;
- Liaison with Buyer assurance functions to aid risk assessment through design and scope review and ensure test coverage and execution covers required risk mitigation and test reporting and that test methodology and resource is appropriate;
- In-sprint testing – QA/automation engineers embedded within development feature teams to prepare and execute system testing against developed features in isolation and develop automation capabilities and frameworks to deploy throughout route to live;
- Integration & E2E Test – prepare and execute end-to-end functional tests against the defined scope of the release within the boundary of the Solution. Support E2E functional and non-functional testing of the Service of which the Solution forms part, for example as required to test E2E contact tracing. The Supplier will liaise with external parties where changes to the Solution impact the data sent to or received from a component outside of Supplier's direct control and scope. This testing includes using smartphones with physical printed and digital simulated barcodes for testing. Additional coverage will be achieved through use of the [REDACTED] tool to allow remote access to a wider range of mobile devices, browsers and connection speeds for compatibility testing.;
- Regression Testing following change, ensuring functional and non-functional performance of the Solution;
- Performance Testing – this testing will test against agreed volumes and beyond to understand whether the platform can support the required volumes of appointment bookings and test centre subject journeys against a set of NFRs to be agreed through the TDA. Such testing shall include appropriate soak and integrated NF testing and regression testing following application or platform changes;
- Cyber Security Testing – static code analysis;
- Cyber Security Testing – authorised simulated cyberattack to identify exploitable vulnerabilities against a defined scope of the Solution;
- Operational Acceptance Testing (OAT) – testing to verify that the operations team are able to provide the Solution and confirm key aspects of the serverless infrastructure is in place (alarms, dashboards, /monitoring, backup, disaster recovery and business continuity);
- Test Summary Reports – test summary reports will be produced per release to production and made available to the Buyer on Confluence. The report will describe the testing undertaken, the results of the testing, and any outstanding defects that remain at the end of testing for the release and test limitations and exclusions; and
- Participation and collaboration with Buyer stakeholder approval and other assurance activities, including Buyer approval forums.

Service 3: Cyber Security Technical Services

The Parties acknowledge the Supplier has a responsibility to apply and comply with Cyber Security Requirements for the Solution. If any ambiguity on the Supplier's responsibility to apply or comply with

the Cyber Security Requirements is identified by either Party, that Party will notify the Security Working Group for discussion and resolution.

Based on authorised and prioritised business requirements, and in parallel with the design, development, testing and operation activities of the Solution, the Supplier will configure, apply and operate the Cyber Security Requirements.

The primary governance forums for the discussion, selection, prioritisation of cyber security controls, cyber security designs and cyber security configurations, and the Cyber Security Requirements are the governance forums listed in Section 5, specifically the Technical Design Authority and Security Working Group. The authority for any exception(s) to or deviation(s) from the Cyber Security Requirements is solely with the Security Working Group.

The appropriate cyber security governance forum (listed in Section 5) reviews any such Cyber Security Requirements, risks and controls, and if necessary, determines priorities or exceptions to any requirements, standard, framework or control.

The Parties will participate in the primary governance forums as a matter of course, where the Buyer may review the selection, prioritisation and design of security controls. The Buyer may request adjustments to the Cyber Security Requirements or specific controls, recognising the potential for impacting existing or proposed development, testing or operational activities.

The selection and application of any specific individual or collection of cyber security controls is considered by the Parties in the context of risk(s) to the Solution, legal or regulatory obligations, and impacts to either the development or operation of the Solution.

The Buyer is the accountable party for determining the necessary and sufficient mitigation of cyber risk to their satisfaction. The Supplier will comply with all reasonable request in relations to audits relating to the Services, whether being carried out directly by the Buyer or by the Buyers nominated third party.

Cyber Security Requirements are defined under the Glossary set out in the Order Form , and may be informed by external guidance from the NCSC or other government departments, and good practice guides, including but not limited to:

- Centre for Internet Security configuration guides;
- OWASP SAMM and ASVS;
- NHS D Cloud Good Practice Guide; and
- NCSC End User Devices Platform Guide, NCSC TLS External Facing Services.

The Supplier will:

- Maintain an ISO27001 certification for the scope of its day to day business operations. The scope need not include the Solution, in part or whole;
- Apply the Cyber Security Requirements to its direct and immediate Subcontractors, to the extent possible by reasonable efforts. Any material exception to this will be brought to the Security Working Group for consideration and approval;
- Support reasonable and timely requests for information, or assurance activities;
- Work with the Buyer to define and establish and maintain a cyber security and data privacy risk register;
- Create and maintain a controls register, and provide regular reporting to the Security Working Group. The scope, detail and format of the register and reporting are to be decided by the Security

Working Group;

- Apply cyber risk mitigations at the request of the Buyer, with the Buyer recognising the potential for impacting existing or proposed development, testing or operational activities;
- Establish and maintain a Risk and Threat Model, based on good practices to inform the selection and prioritisation of security controls;
- Conduct security testing, including but not limited to static code analysis, vulnerability analysis, and authorised simulated cyberattacks with a defined scope ("**Pen Testing**"). The frequency and scope of testing, and timescales for remediation will be agreed by the Security Working Group. Specific remediation plans will be prioritised based on risk (score based on industry practice such as CVSS), and business functionality priorities;
- Maintain a register of identified vulnerabilities and remediation activity, and make this available to the Security Working Group;
- Provide a Cyber Protective Monitoring Service – as per section 3.1;
- Be responsible for the Supplier's corporate and physical security of all assets under its physical control that provide services for the Solution;
- Document and maintain the scope (i.e. the assets at risk which require mitigation) of the Cyber Security Requirements. Bring any identified potential new or ambiguous cyber scope to the Security Working Group for discussion and resolution; and
- Identify material data assets, create and maintain a Data Asset Register. The register will specify the agreed retention period(s), encryption standards for transmission or storage (if any), and agreed methods or standards for data erasure and/or data archival.

The Supplier will not:

- Be responsible for the Buyer's Corporate Security or Physical Security, or physical elements of cyber security of the Buyer or the Buyer's other service providers.

In complying with the Cyber Security Requirements, the Supplier's activities shall include but are not limited to:

- Apply Identity and Access Management (IAM) good practices to protect Buyer Data, noting the distinction between IAM for (1) the Supplier and authorised third-parties, and (2) end-users of the Solution;
- Follow the Buyer's processes for raising and managing cyber security incidents, and integrate as required with nominated stakeholders;
- Implement and document cyber security and data privacy awareness training for its employees within the scope of the Services;
- Apply and maintain good practices and training on secure software development lifecycle;
- Implementation of a requirements-driven security testing regime to support assurance and acceptance of service and application releases;
- Improvements to security network segregation through improving network perimeter security (including content inspection and web application firewalls);
- Development of business continuity and disaster recovery plans, including exercises to identify and uplift shortfalls with specified Buyer service levels;

- Review cyber incident response processes and playbooks, integrating with the Buyer incident management and uplifting SLAs in line with Buyer requirements;
- Support with the identification of relevant industry and regulatory standards related to data protection and working with the delivery teams across the Supplier, the Buyer and DHSC to ensure these are evaluated, documented and implemented across the programme in line with risk appetite;
- Overseeing change management activity to ensure the Supplier's responsibilities as a data Processor are followed and relevant artefacts (such as data processing agreements and data flow diagrams) are maintained and sustained throughout change activity; Supporting with the Buyer and DHSC Information Governance teams to identify, articulate and evaluate data protection focussed non-functional requirements in response to new functional requirements for the platform; and
- Identification of resilience and recovery improvements in third-parties associated with the Solution and contracted to the Buyer or DHSC.

Service 3.1: Cyber Security Protective Monitoring Services

The Supplier's Protective Monitoring ("PM") service analyses event logs generated by the Supplier hosted [REDACTED] environment that is used to deliver TTCE capability in order to detect indicators of malicious activity, for agreed use-cases.

This is achieved through the collection and analysis of the log event data generated. Events are collected into a central location (SIEM and analytics platforms) and algorithms are run over this data to identify activity that warrants further investigation. The Supplier's analysts review this activity, and raise incidents to the Supplier's [REDACTED] teams for resolution, whilst also informing the NHS CDOC.

[REDACTED]
[REDACTED], which includes the activities to on-board the Solution, conduct the ingestion of information, analysis, triage, and integration with and reporting to defined Buyer service and cyber incident desks. [REDACTED]
[REDACTED]
[REDACTED]

The Supplier will provide this Service in accordance with the service levels as set out in Section 3 of this Order Form Schedule 1. The monitoring shall cover all relevant services defined and agreed between the Supplier and Buyer, and include both the supporting infrastructure and the application itself. The Supplier shall undertake to collaborate with the Buyer to integrate all security protective monitoring, alerting, and supporting activity within the Buyer CDOC and CSOC processes. This includes identifying assets and services that require monitoring, establishing monitoring use cases, defining and implementing monitoring playbooks, and any other activities that may arise. The exact nature of the requirement in this area will be informed by CSOC and CDOC stakeholders and will require cooperation between Supplier and Buyer to define, but may include establishing monitoring playbooks for Supplier Staff to carry out, with associated alerting and escalation to the Buyer, or may include direct ingestion of security event data by CDOC and CSOC as appropriate, with support from Supplier Staff.

The Supplier will also provide Threat Hunting over the collected data. Threat Hunting is where analysts will proactively query the data collected to identify potential attacks that were not detected by operational monitoring. Supplier and Buyer stakeholders will need to agree threat hunting playbooks to ensure that the relevant risks identified by the Buyer are subject to appropriate security analysis.

The Buyer will have final discretion over the scope and nature of the security monitoring and Threat Hunting activities that are undertaken.

It is acknowledged that Buyer requirements for security protective monitoring services may evolve over time, this could include a target state where the CDOC / CSOC on-boards some or all of the Services delivered in accordance with this Call-Off Contract. These determinations will be driven by the Buyer and will require cooperation and participation from the Supplier to facilitate any future changes to the delivery model for security monitoring.

Service 4: Data Visualisation (MI Platform)

This Service will only be provided under this Call Off Contract until the 31st August 2020.

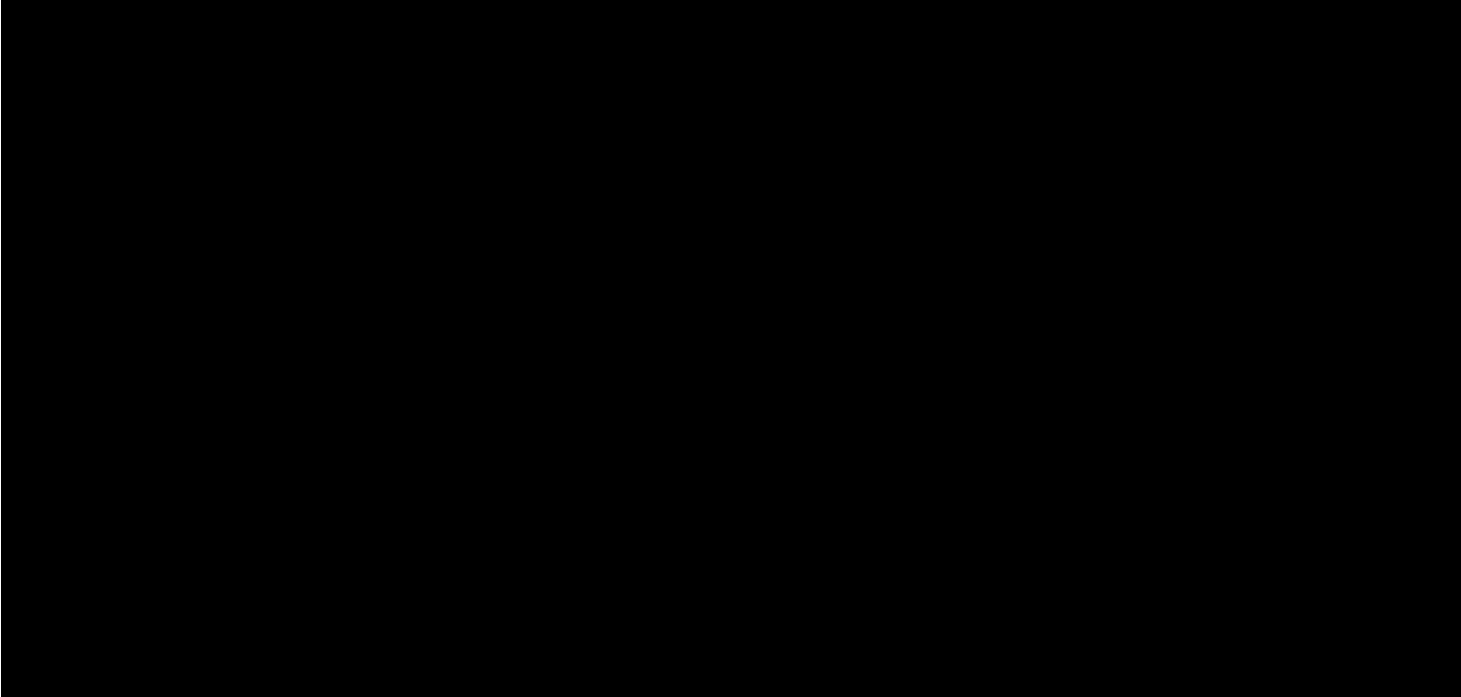
This Service delivers the Management Information (MI) Platform using functional and technical services. It also supports a hub and spoke model that engages and empowers individual MI designers in other programme areas. Specific reporting requirements will be managed and prioritised by the Buyer in accordance with the governance set out in Section 5 (Governance) to this Order Form Schedule 1.

The Services included:

- Data Modelling – developing a fact table based data model that supports expressive, but simple, MI querying;
- ETL development – constructing [REDACTED] based ETL pipelines to satisfy the data cleansing and joining requirements of the data;
- S3 Bucket Maintenance – standing up S3 buckets and associated cyber constraints to support data drops from third party systems;
- Platform Administration – on boarding and troubleshooting for the platforms end user base;
- Testing – including UAT, Penetration and Performance testing;
- MI Development – build of dashboards satisfying programme MI requirements, including KPI definitions, statistical quality review; and
- Data Dictionary Development – build and maintenance of dictionary artefacts.

[REDACTED]
[REDACTED]
[REDACTED] This migration shall be effected through a formal Variation to this Call-Off Contract. MI Platform architecture and data scope.

The MI platform currently combines data staging and data visualisation. Consensus has been arrived with DHSC and NHSD to further decouple the product, breaking the platform into a Staging Platform (DPS) and a [REDACTED] Visualisation Platform (DHSC), with both leveraging the existing MI Platform assets. Furthermore, the Staging Platform will migrate into the NHS D DPS [REDACTED] estate.



These data sources will be sent via SFTP or direct API connections and stored within [REDACTED] buckets. They will be connected using available unique identifiers (expected to be QR code, in addition to additional third party identifiers such as [REDACTED] ID) to provide a comprehensive fact table view, to provide a complete end to end view of a given test instance. The [REDACTED] buckets are currently hosted on Supplier cloud infrastructure. During the Term of this Call-Off Contract, these [REDACTED] buckets will migrate to the Buyer's cloud infrastructure. This migration shall be effected through a formal Variation to this Call-Off Contract.

In order to preserve privacy, a tiered architecture is being developed, which limits the access to record level data to only those users (and use cases) that can justify a need for record level information:

- Tier One contains the [REDACTED] buckets, where raw data is held, with ETL jobs rejecting any overt PII information (in addition to other DQ checks);
- Tier Two contains the connected record level data sets; and
- Tier Three present Tier Two in an aggregate, privacy preserving, form, typically accessed via tableau, but also analysed via [REDACTED] and [REDACTED].

Service 5: Salesforce Cloud Services (Satellite Manager Ordering Portal)

This Service provides enhancements and live operations for the existing Salesforce Cloud Service which allows bulk ordering of test kits (initially for care homes but extendable to other organisations), and assistance for back office processing of these orders and analytics and reports.

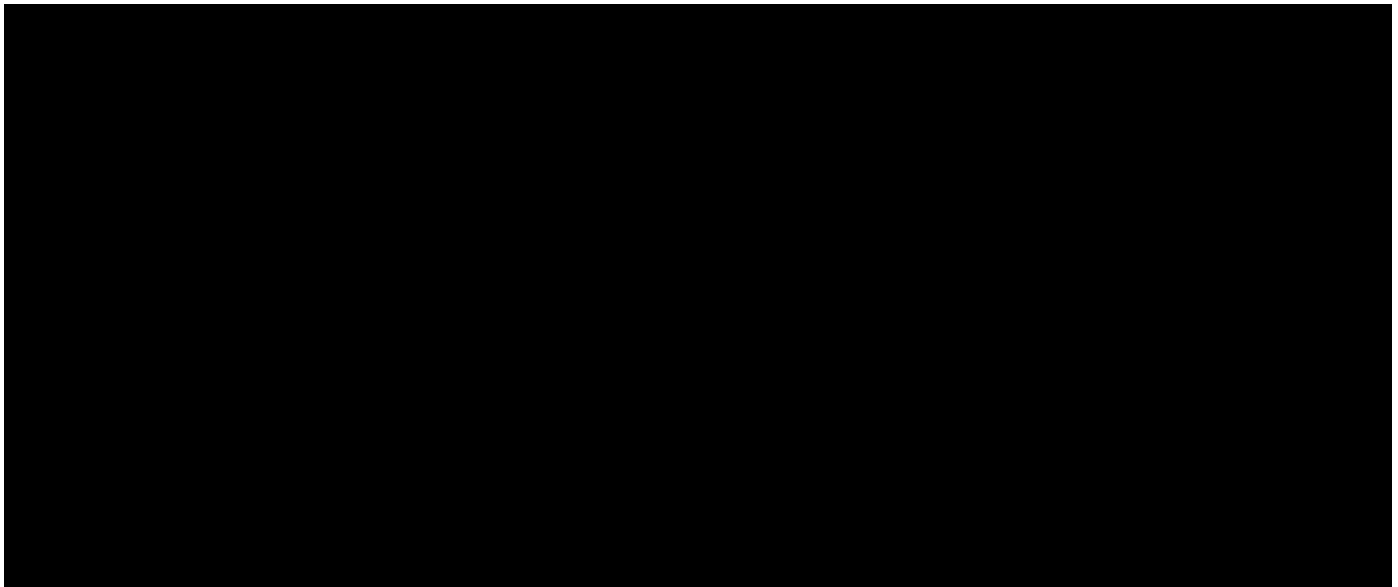
This Service is delivered by an integrated team that has a dedicated design, build, test and live operations team.

The Service includes:

- Support the prioritisation of the Buyer's product roadmap including functional and architectural impact assessments of enhancements;
- Develop the end to end journey for bulk ordering of test kits with support from the Buyer;
- Architecture and technical design for enhancements to this part of the Solution;

- Functional design, business analysis and UX design;
- Support for the NHS Digital Assurance activities for example clinical, security, information governance, and solution assurance;
- Salesforce Cloud implementation including front end development, custom code and Salesforce platform configuration;
- Functional and non-functional QA testing of the new enhancements to the platform;
- Design, build and maintain the non-production and production environments;
- Development of fixes for defects identified by the QA testing;
- Release management and documentation of release artefacts to deploy code and releases to the non-production and production environments, and participate and collaborate with the Buyer's assurance processes (e.g. CAB); and
- Analytics and reports that support management information and Buyer decision making for the Service.

The architecture for the [REDACTED] Service is shown below.



Buyer responsibilities for Service 5:

- Manage the mailbox which includes (but not limited to) queries about care homes test kits (orders, deliveries, issues, questions); and
- Providing information and guidance on test kit usage by organisations or subjects for example how to order test kits and how to use the test kits (a) evaluating the adequacy and results of the services performed including approving and adopting any resultant projections provided that such results are submitted by the Supplier in an appropriate form to enable evaluation.

Assumptions applicable to all Services:

- Given the exceptional circumstances of Covid-19 and the requirement to be flexible and responsive in how the Supplier provides Services to the Buyer in dealing with the Covid-19 situation, the Parties will work together in good faith to manage the scope of the Services provided

by the Supplier, including any changes in the scope of the Services. Any changes in scope will be pre-agreed via the governance process set out in Section 5 of Order Form Schedule 1;

- The Parties acknowledge and accept the risk posed by the spread of Covid-19 and the associated impact this might have on the delivery of the Services. The Parties' personnel will comply with any restrictions or conditions imposed by their respective organisations on working practices as the threat of Covid-19 continues. The Parties accept that they may be required to adopt alternative working practices and put in place safeguards during this period, including working remotely, restrictions on travel to and from particular locations and the quarantining of individuals; and
- The Supplier's work will be limited by the time available, scope of work and information available to it. As a result of these limitations, the Supplier may not identify all circumstances or information relevant to the Services or that the Buyer may regard as relevant. Whilst the Supplier may review spreadsheets or models provided to it by or on behalf of the Buyer to facilitate understanding, it may not test them for robustness. The Supplier shall highlight to the Buyer any instances where such a test is recommended but cannot be carried out by the Supplier.

Consent required for information sharing

The Supplier shall not share any Buyer Confidential Information with any third party not involved with the provision of the Services without the express written consent of the Buyer's Delivery Leader or Delivery Head as detailed in the Buyer Personnel Authorisation Table set out in Section 6 of this Call-Off Contract. This provision shall supersede those set out in paragraph 8.3 of the Supplier Terms which shall accordingly be disapplied from this Call-Off Contract.

The Supplier shall act with diligence when reviewing data provided by the Buyer and / or when transferring data to the Buyer. In the event any data provided by the Buyer to the Supplier appears to contain inaccuracies or is misleading, the Supplier shall bring such inaccuracies or misleading information to the Buyer's attention using the governance forums set out in Section 5 to this Order Form Schedule 1. This obligation to act with diligence shall supersede and replace the provisions set out in paragraph 4.4 of the Supplier Terms.

Section 3: Service Levels

General:

The end to end business service requirement is that no virus test should take longer than 24 hours from submission to return of results to the submitter. The Supplier will work proactively with the Buyer and other required parties to support this business service requirement.

The Supplier shall provide the following for the Solution within the scope of this Call-Off Contract:

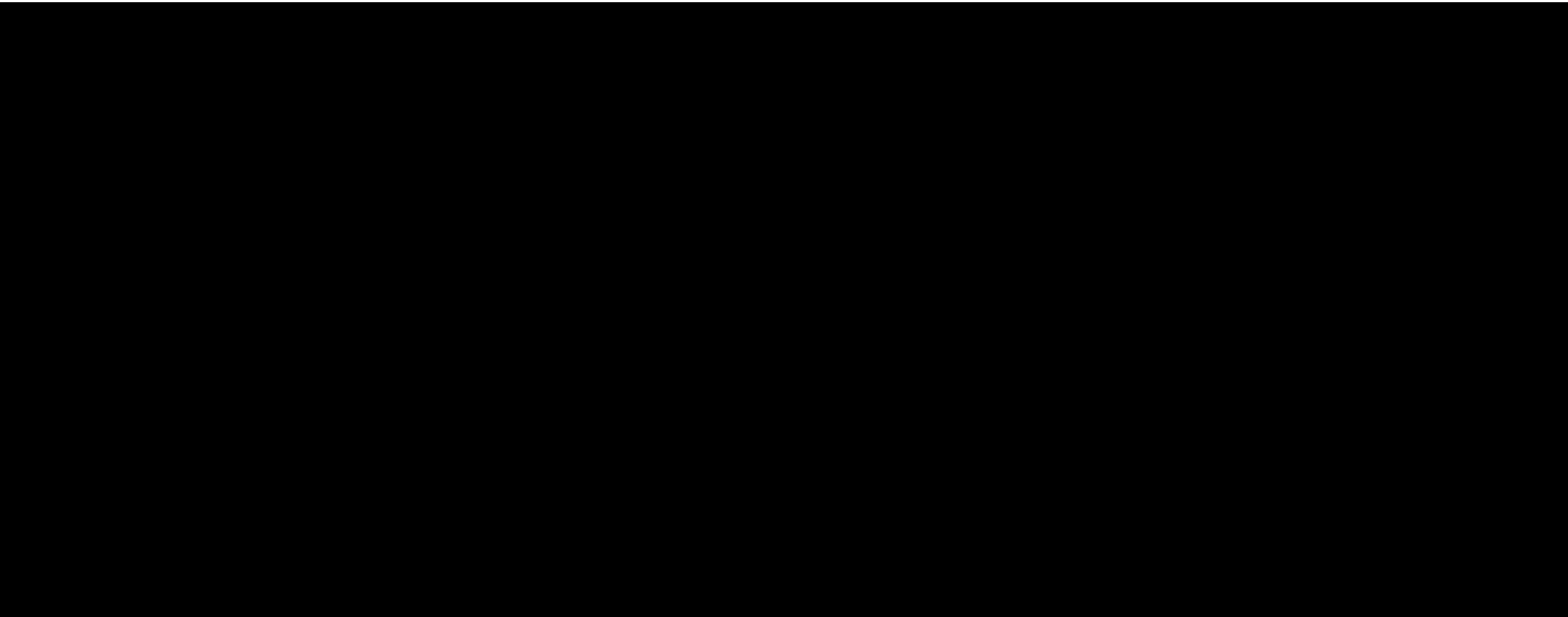
- Run a service desk and service management layer to handle incidents, service requests and problems relating to the Live Running Service (as defined below) during the Hours of Service (as defined below). This is a service for the Callers identified in the scope of the Live Service diagram below, not for the general public;
- Coordinate incidents for [REDACTED];
- Investigate incidents and errors, monitor and respond to alerts about issues impacting the Solution, including the [REDACTED] hosted infrastructure and applications deployed within the infrastructure;
- Participate in the HSSI process for severity 1 and severity 2 incidents only; and
- Hours of service

The Supplier shall observe a standard working day of 09:00 – 18:00, Monday – Friday UK time with the exception of English Public Holidays and the last working day before Christmas (normally 24 December) (the “Working Day”). The Supplier will deliver the Services during the hours of service defined in the following table (the “Hours of Service”):

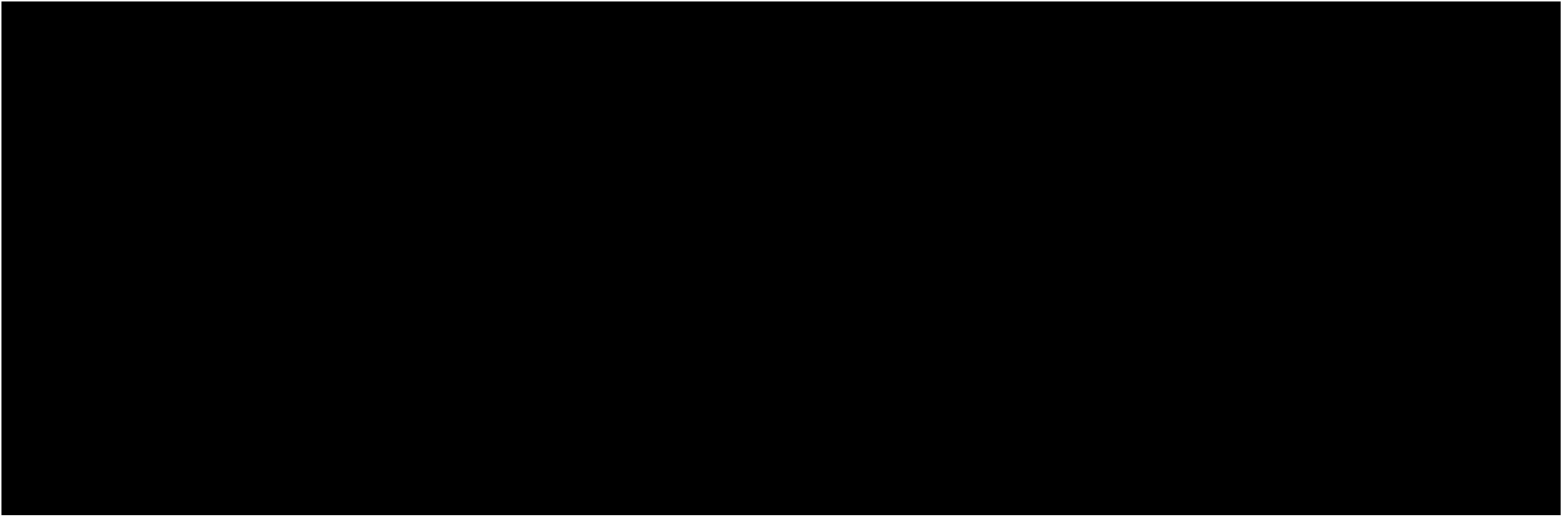
Service	Hours of Service
Service management	Working Days
Live service team	Working Days
Triage and resolution	Working Days: Severity 1 and Severity 2 incident triage and resolution for the platinum Service Tier 24x7 Working Days: Severity 1 and Severity 2 incident triage and investigation for the gold Service Tier 24x7 (For the avoidance of doubt incident resolution if development is required for the gold Service Tier shall be performed during Working Days only)

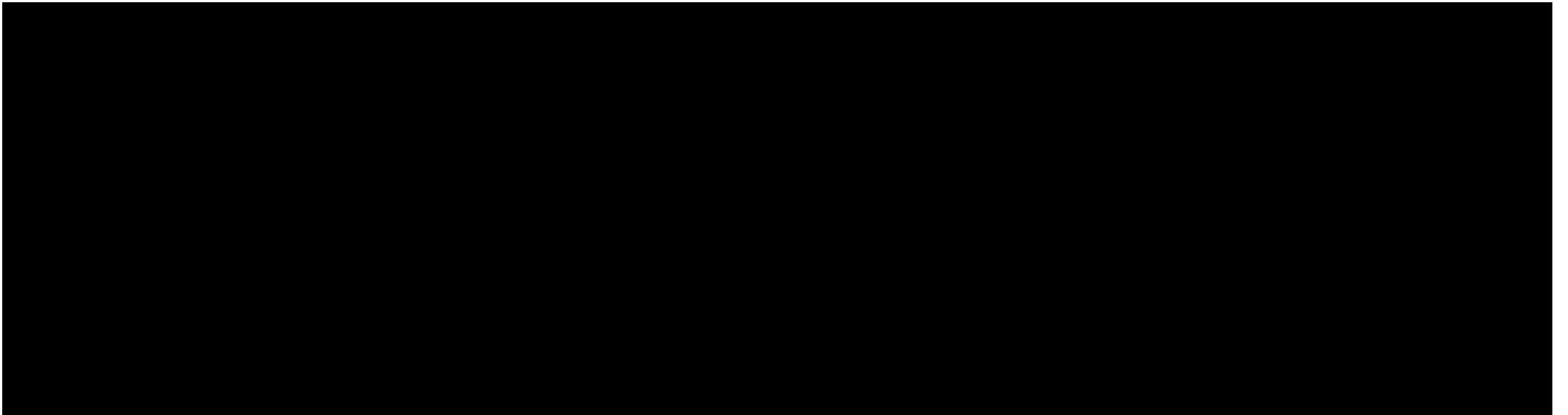
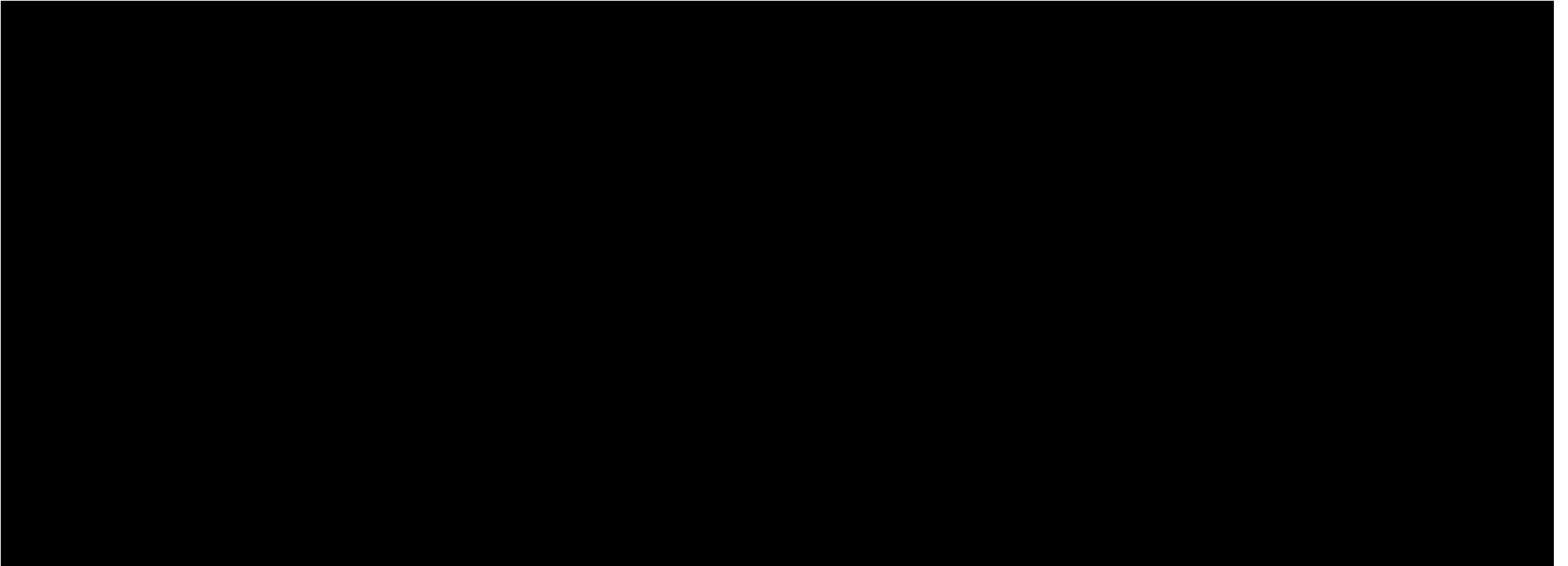
- Prior to any agreement of a full service level agreement the Supplier will use all reasonable endeavours within the agreed resourcing levels to achieve, subject to the Excusing Causes, the Target Service Performance (as defined below). The Supplier shall report monthly to the Buyer on all achievements and all failures in regards to the Target Service Performance at the Call-Off Review Meeting and no changes shall be made to this template unless agreed between the Parties pursuant to and in accordance with the Variation procedure.

The Parties agree that the target service performance shall be the Service Measurement Metrics set out in the Balanced Scorecard for the Live Running Service only, as set out below (the “**Target Service Performance**”):





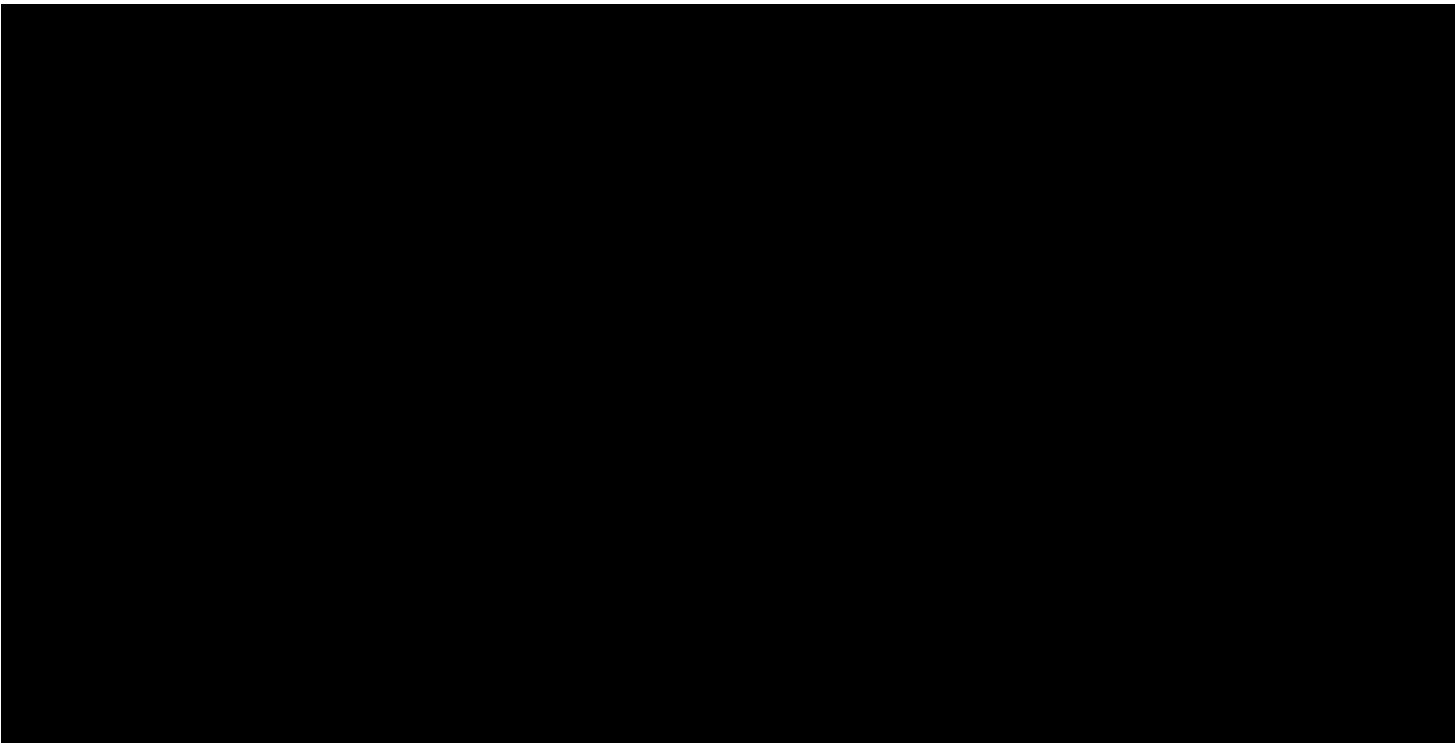




The Supplier shall provide any supplementary information to the Balanced Scorecard that is reasonably requested by the Buyer.

- [illegible]

The scope of the Supplier live service is shown in the diagram below ("**Live Running Service**"):

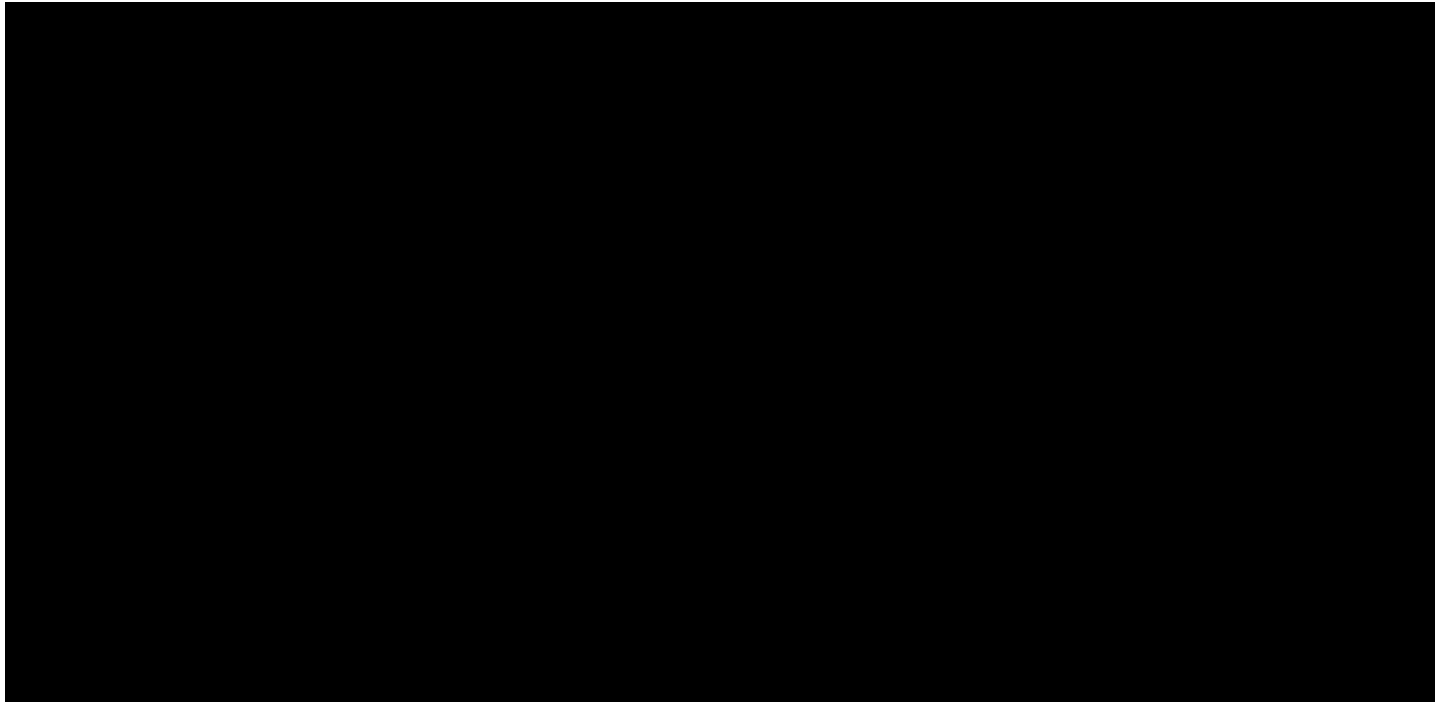


- Service Tiers

The Target Service Performance shall be based on the criticality (“the **Service Tier**”) of the Solution component. The following Service Tiers shall be delivered by the Supplier:

- I. platinum;
- II. gold;
- III. silver; and
- IV. bronze.

- The Service Tiers applicable to the Component Systems in scope of the Live Running Service are shown below:



As per all Services (excluding the Cyber Protective Monitoring Service) provided under this Call-Off Contract, [REDACTED]. The team size may need to be increased if the number of service requests, incidents or volume of calls to the service desk

increases. These metrics will be reviewed with the Buyer regularly and actions agreed, which may include increases to the team size in accordance with the Governance.

Full Service Level Agreement (subject to Variation)

The parties shall work in good faith to agree a fully defined service model relating to the Live Running Service elements of the Solution. This defined service model will include a defined service level agreement and shall be incorporated within the Call-Off Contract by Variation and may include, but not be limited to, the following:

- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

This fully defined service model shall not remove the Supplier's obligations (except those in relation to the Target Service Performance) for the purpose of the Call-Off Review Meeting set out in paragraph 5 of Section 5 (Governance).

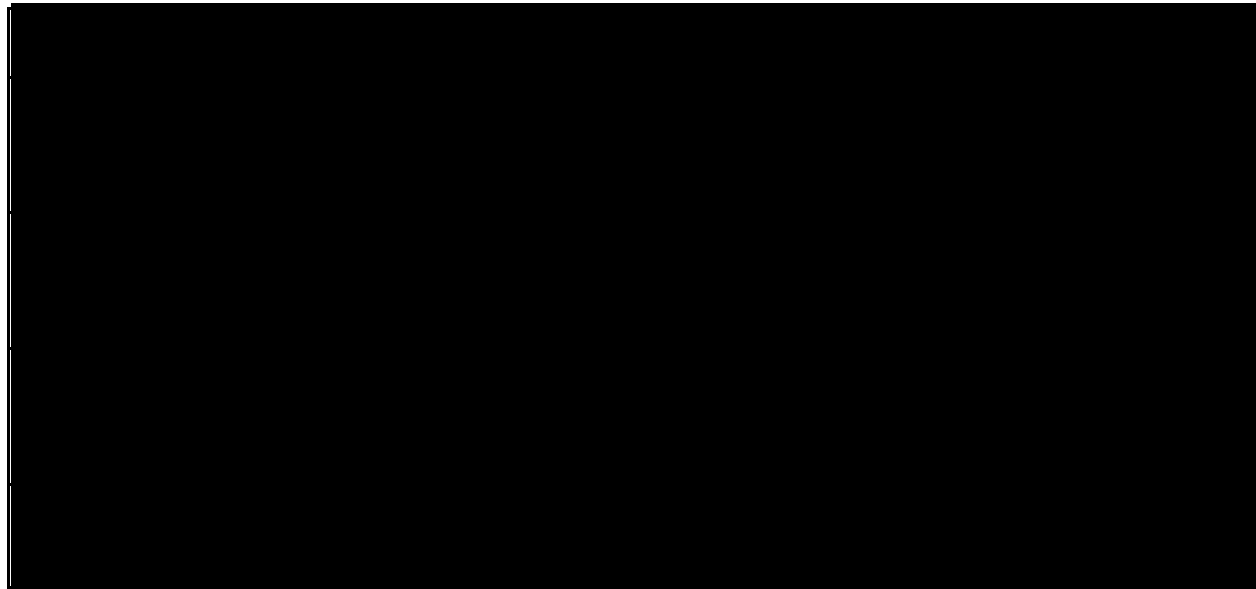
Service Levels for Service 3.1: Cyber Security Protective Monitoring Services

The Supplier will consume event data from the TTCE environment in scope, perform automated analysis and perform initial triage for all potential incidents identified 24x7x365. This needs to feed into CDOC monitoring in accordance with requirements specified by the Buyer, according to Buyer templates and requirements for ingestion into the Buyers monitoring services. Where an incident is considered to have a potentially Critical or High priority then these will be investigated 24x7x365. [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

The Supplier commit to the following service levels :



The above severity description are subject to further review and amendment by the Buyer.



Additional Service Levels for Service 5: Salesforce Cloud Services (Satellite Manager Ordering Portal)

Operation of the live service to handle incidents, triage and problems relating to the live service between the hours of 9am and 6pm Monday to Friday. This is provided for the Buyer’s staff not general public.

Section 4: Supplier resource allocation;

The Supplier shall deliver the Services using the following team structures. These may be varied via the Governance as set out in Section 5 to Order Form Schedule 1.



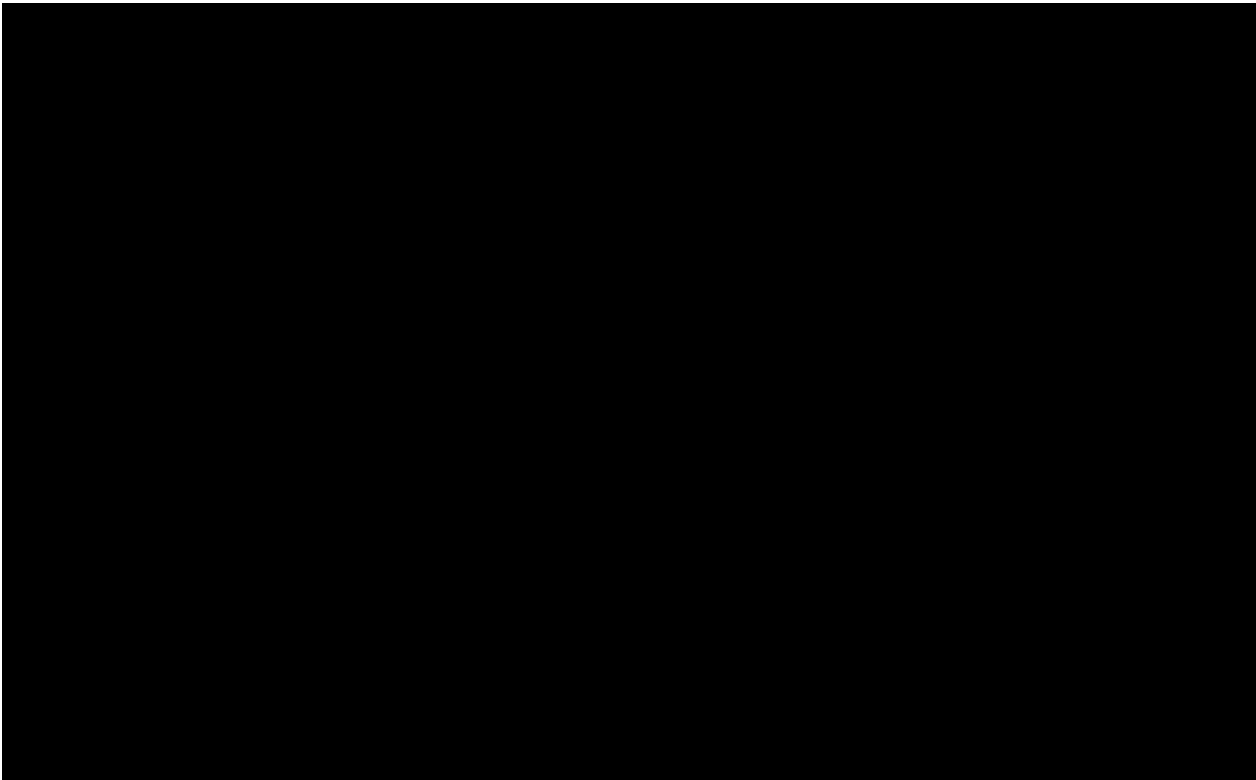
Description of services	Call Off Contract ref:
Leadership and management - this is the senior team that manages the delivery programme. Delivery is where most time is spent, but this team also coordinates with the wider programme, engaging with all the different parts of DHSC and NHSD, including assurance, governance, planning, finance. It manages the teams described below.	Service 1: Cloud Technology Transformation Programme
Cloud architecture and design – is the product/UX and technology architecture team. They work closely with your product management team and your architecture governance, helping to shape the roadmap items, executing UX, copy, subject journey design, and preparing architectural designs for the factory, which consumes the design and executes lower level technical design and requirements elaboration.	Service 2.1: Cloud architecture and design
Factory – these are the teams that take designs from the Cloud architecture and design team, add detail, and then develop and test them to produce realized features. Currently there are teams for: Individual based testing, mobile and admin portal, organizational based testing, and core data and resilience. The teams are multi-skilled and include scrum master, BA, UX, development, platform, QA (incl. automation testing). If there is a requirement to address a new area or increase capacity this can be addressed given reasonable notice via the Governance.	Service 2.2: Cloud hosting, infrastructure and application planning and delivery
Integration and NF testing — this team executes integration testing, penetration testing, performance, and OAT on the Deloitte factory output.	Service 2.3: Cloud testing
Platform and service management – this is the team that manages all of the non-production and production environments, and the deployments between them all, as well as live operations.	Service 2.2: Cloud hosting, infrastructure and application planning and delivery

MI platform – This is the team that is implementing the strategic analytics/tableau platform, and developing reports and dashboards for the business and migrating the staging platform and tableau assets to DPS and DHSC respectively.	Service 4: Data visualisation (MI Platform)
Bulk ordering (salesforce) platform – this is the team that has implemented Salesforce to provision care homes bulk ordering and is implementing a roadmap of enhancements.	Service 5: Salesforce Cloud Services (Satellite Manager Ordering Portal)
Cyber support – comply with the Cyber Security Requirements	Service 3 – Cyber Technical Services
Cyber Security Protective Monitoring Service	Service 3.1 Cyber Security Protective Monitoring Services
Cloud costs [REDACTED] and tooling – these are the cloud costs and tooling.	Third party toolsets

Resource Numbers

In order for the Supplier to provide the full lifecycle of the Services the following resources are provided as part of the above teams:

- Developers (front-end engineers, back-end engineers, data engineers, tech leads)
- Testers (automation test developers, exploratory testers, penetration testers, accessibility / user experience testers)
- Business Analysts (functional designers, story writers, product managers, business relationship managers, accessibility analysts)
- Designers (researchers, service designers, visual designers, experience designers)
- Architects (technical architects, data architects)
- Security (data privacy, cyber experts, security operations, security architects)
- Delivery Leadership (delivery leads, release managers, team leadership, PMO)
- Service & Platform Operations (DevOps, platform engineers, service managers, service operations)
- Commercial (service level managers, legal / regulatory, contract manager)



The number of resources allocated by the Supplier to provide the Services are forecasted as shown in the table below. Note that these are estimates. The Cyber FTE detailed in the above table excludes the Cyber Security Protective Monitoring Service which is provided as a managed service.

The above total provision of [redacted] resources will be defined as the **'Resource Baseline'**.

Any increase to this Resource Baseline must be agreed via the governance process set out in Section 5 of this Order Form Schedule 1.

[redacted]
[redacted]
[redacted]

- I. [redacted]
- II. [redacted]

In the event that either or both of the above volumes are exceeded, the Parties may agree to proportionally increase the Resource Baseline and the Charges in accordance with the governance process set-out in Section 5 (Governance) to Order Form Schedule 1 of this Call-Off Contract.

Section 5: Governance;

The Parties recognise that the delivery of the Services need to be governed in the following manner:

- 1. [redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

2. **Solution Development:** The Parties shall work together to agree a monthly Development Solution Roadmap, capturing functional and non-functional changes to the Solution. These will be approved by the parties and captured in the COVID 19 Testing Development Priorities on a monthly basis ("**Priority List**"). This will be formally agreed between the Buyers Product Manager and the Supplier on a monthly basis, or more frequently as required by the Buyer (acting reasonably). [REDACTED]

July COVID 19 Testing Development Priorities attached:

[REDACTED]

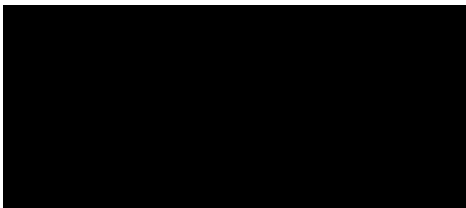
This is a target set of items, and the Supplier does not undertake to deliver all these items within the indicative timeframes. The size and complexity of some of these items is unknown and therefore where larger or more complex than anticipated, scope and/or complexity will need to change. The target set of items are reviewed every week and can be reprioritised and/or items removed or inserted by mutual consent. The parties acknowledge that defects and errors are a normal part of software development. The parties may use this process to prioritise and fix defects and errors as part of the backlog prioritisation process.

- [REDACTED]
3. **Resource and Charges Control:** The Parties recognise that there needs to be close control over both the size of the Supplier teams and cumulative spend against this Call-Off Contract in providing the Services.

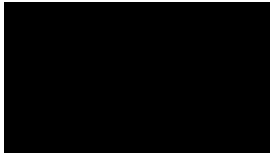
- a. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- b. **Team Variation:** The Buyer will schedule and the Parties will meet on a weekly basis to discuss and agree [REDACTED].

[REDACTED]



The Supplier will provide a current dashboard in accordance with the following template to support these weekly meetings:



- c. **Charges:** 

 (**Charges Forecast**).

The Charges Forecast will provide for each resource following:

- Name
- Grade
- Allocation to which team and Service
- Charges
- One line role description
- Location (remote or office-based)
- Supplier line manager
- Buyer line manager/owner under Buyer Personnel Authorisation Table

Other known risks that may impact costs will be highlighted alongside the forecast.

Each month the Call-off Review Meeting will review the Resource and Charges forecast and actuals, and any approvals or corrective action agreed.

4. **Call-off Review Meeting.** The Buyer will run a monthly meeting to review the performance of the Supplier's Services and the Charges forecast. Each month, the Supplier will provide a pack for the meeting that will include:

Services review:

- a. Description of deliverables and value delivered (no less detailed than provided for the deep-dive review);
- b. Description and metrics on quality;

- c. Description and metrics on velocity (throughput);
- d. Description of platform and service management (in accordance with the Target Service Performance as set out in Section 3 (Service Levels) above;
- e. Review of dependencies and obligations; and
- f. Proposed action plan for discussion for Supplier and Buyer where corrective or improvement is needed (this may include areas for the Buyer to address) in any of the above areas.

Charges:

- a. [REDACTED]
- b. [REDACTED]
- c. Proposed action plan for discussion if needed.

The output of the meeting will be a record of deliverables, value delivered, quality and velocity, the forecast and actual charges, and an action plan where corrective or improvement is needed. This process needs to be completed prior to the Supplier raising any invoice for payment for that month. [REDACTED]

The meeting must be attended by the following key roles: Supplier Partner and Buyer Delivery Leader.

5. Approval of Supplier Claims;

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

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

The Parties acknowledge and agree that the provisions set out in paragraph 5 of the Supplier Terms relating to testing and acceptance shall not apply to this Call-Off Contract.

Project Roadmap: The Parties shall address the following areas of project development. The Supplier shall provide its full participation and collaboration in achieving the following tasks in a reasonable timeframe. In order to support the Supplier in meeting its obligations under this paragraph 6, [REDACTED]

- a. [REDACTED]

- c. Supporting a full evaluation and assurance of the Solution design by the Buyer;
- d. Establishing service level agreements across the whole Solution;
- e. [REDACTED]
- f. Transition of Infrastructure, hosting and third party contracts to the Buyer or the Buyer's nominated party. The Supplier was engaged by the Buyer to provide a complete service for the Solution therefore some of the environments and tooling (for both development and production) are on Supplier-owned cloud infrastructure. It is the intention of neither the Supplier nor the Buyer that the Supplier continues to own the infrastructure and tooling in the long run, and a migration plan should be developed accordingly;
- g. Construction of tender documentation and requirements for competitive tender of the Solution and Services; and
- h. Provision exit support to allow a smooth transition of Solution management and Services at the end of this Call-Off Contract.

[REDACTED]
[REDACTED] The current set of forums in place are (terms of reference to be provided by the Buyer and agreed between the parties):

- Digital leadership team meetings which is the top level decisions making forum on scope, planning and prioritisation. [REDACTED]
- Technical Design Authority (TDA) which makes decisions on the architecture and technology.
- Product Management which determines requirements and priority. This forum will review the COVID 19 Testing Development Priorities.
- IT quality and clinical assurance which determines whether the design or implementation of the design is acceptable from an IT quality and clinical assurance perspective.
- CAB (IT Change Approval Board) determines whether a release is approved for deployment into production.
- Information Governance
- Daily content change prioritisation meeting
- Regular (no less than monthly) Service Level performance reviews
- Weekly Security Working Group forum
- Weekly release overview meetings with the NHS Digital Assurance team
- Call-off Review Meeting
- Security Working Group (SWG)

The frequency and scope of the governance forums may be changed by mutual consent between the Supplier and Buyer. [REDACTED]
[REDACTED]

Section 6: Buyers Responsibilities;

The Buyer shall (on its behalf and as agent for the Third Party Beneficiaries) be solely responsible for:

- Defining all Solution requirements including the Cyber Security Requirements;
- Participating in all Governance forums. Leading the Security Working Group and Information Governance forums;
- Policy decisions for example decisions on which organisations or subjects are eligible for testing, or the volume of test kits that care homes should receive;
- Providing high level requirements and responsibility for ensuring the requirements meet the needs of the user;
- Business change execution to ensure the features developed by the Supplier are successfully understood, used, and embedded within the intended users;
- Operational processes for example, defining and setting up an effective organisation, people and processes to use the Solution;
- Supply chain for example, supply of test kits, including ordering, warehousing, picking, distribution, and postage/delivery, collection, testing, and lab testing and communication of test results;
- Demand planning and forecasting of volumes that the Solution needs to support, for example volume forecasting for expected numbers of subjects per channel or region;
- Verifying the Cyber Risk and Threat Model is sufficient to manage their business risk decisions;
- Determining (as necessary) and notifying the Supplier in writing of protectively marked Buyer Data held or processed by the Solution. The Buyer acknowledges any such notification may impact development, testing or operational priorities;
- Providing the Supplier with accurate and complete information, retaining sole responsibility for data and assumptions used in the preparation of analysis or development or QA/testing;
- Where it is agreed that Supplier personnel shall work from Buyer premises, providing all necessary office space and equipment, IT systems access, internet connectivity and ancillary facilities;
- The Buyer will provide management decisions in a timely manner and arrange for a delegate for any period of absence;
- The Buyer will have full and sole responsibility for the accuracy, appropriateness and legality of all forms, text, copy, guidance and other content. The Supplier will rely upon the Buyer's designated Product Owner/Manager(s) and Delivery Leadership to provide guidance;

- Save as expressly provided for in the Call-off Contract or agreed otherwise, the Buyer will be responsible for all procurement of nonstandard software, hardware and licenses required to develop, test and operate the Solution, subject to a list being agreed in advance with the Buyer;
- The Buyer will take responsibility for any business change and staff training that may be required in order to deploy the services into live usage, and to realise the desired business benefits;
- The Buyer will agree appropriate data processing agreements (and the Supplier will support the Buyer in preparing its DPIA and Transparency Notice). The Supplier will comply with all reasonable requests for information;
- The Buyer is responsible for clinical decision making and clinical assurance of the design and realisation of the design, including the decision to deploy into live service;
- The Buyer will take responsibility for required changes to other systems including the implementation of required changes to gov.uk, NPEX;
- The Buyer will take responsibility for defining the business and technical architecture within which the Solution is delivered, working in collaboration with the Supplier and taking the Supplier's expertise and advice into reasonable consideration when making architectural choices;
- The Buyer will take responsibility for defining and implementing any "Assisted Digital" strategy;
- The Buyer will ensure that Deliverables that are delivered by the Supplier in a timely manner are reviewed and approved by the Buyer in a timely manner;
- The Buyer will be responsible for managing its own staff and its own third party suppliers effectively and in accordance with the provisions of this Call-Off Contract;
- The Buyer will provide access to third party suppliers as reasonably required to support the required plan and activities;
- Each Party will notify the other as soon as it becomes aware that any assumptions or information that the Supplier is relying upon become invalid or are no longer accurate;
- Each Party will inform the other if it becomes aware of any circumstances or events which will or are likely to impact the provision of the Supplier's services within the anticipated timescales;
- The Buyer will liaise with all other interested stakeholders as necessary (including but not limited to responding to Parliamentary Questions, and responding to audits and reviews by bodies such as IPA and NAO);
- The Buyer will obtain appropriate legal, technical or other specialist advice for systems or processes outside the Supplier's scope to deliver, where this is required;
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]; and
- The Buyer is responsible for ensuring the Supplier is made aware of the Solution non-functional requirements (NFRs) so that the Supplier test approach and execution are appropriate for the expected demand on the Solution in live operation.

The parties agree that the Buyer responsibilities set out in this Section 6 of Order Form Schedule 1 shall supersede and replace the provisions set out in Schedule 1 to the Supplier Terms. Only those Buyer

responsibilities set out in this Section 6 shall apply to this Call-Off Contract and Schedule 1 to the Supplier Terms is hereby disappplied.

The Buyer is responsible for providing the following operational points of contact to provide authorisation and instructions to the Supplier that shall enable it to manage the delivery of the Services. The named individuals may be changed by the Buyer, giving written notice to the Supplier. The individuals may delegate (in writing on an occasion by occasion basis) their responsibility to direct reports. Except for the Delivery Leader role, the roles are not authorised to make decisions that directly or indirectly increases the [REDACTED] unless the Governance set out in Section 5 of this Order Form Schedule 1 expressly authorises them to do so.

Buyer Personnel Authorisation Table:

Organisation	Role	Responsibility	Current personnel	authorised
NHSD	Delivery Head	Head of the programme for the Buyer.	[REDACTED] [REDACTED]	
NHSD	Delivery Leader	Leading the programme for the Buyer and representing the project at internal governance forums. Supporting the resolution of risks and issues affecting Supplier's delivery. Authorised to increase the Resource Baseline, and agree changes to the scope or structure of the Services with the Supplier.	[REDACTED]	
NHSD	Service Operations Lead	Authorised to review the Supplier Service Operations performance against the Target Service Performance and work with the Supplier to develop proposed a full service model KPIs and SLAs required for live service of the digital platforms.	[REDACTED]	
NHSD	TDA Chair	Technical Architect for architectural and technology decisions for the digital solution. Authorised to agree technology and architecture and data decisions with the Supplier.	[REDACTED]	
NHSD	Product Manager	Defines and prioritises all requirements for the Supplier authorised to agree and prioritise functional and non-functional requirements for the Supplier to build.	[REDACTED]	
NHSD	IT Change	Approval to accepts Supplier's	Operational	change

	Approval Board	release into live service.	procedure (such as the Change Control Board – terms of reference as defined by the Buyer)
NHSD	Security	Authorised to set the overall security policy for the Supplier.	██████████
NHSD	Information Governance	Policy lead for NHSD Information Governance which includes data privacy. Authorised to set standards for information governance sand privacy.	████████████████████
NHSD	Data & MI Lead	Responsible for integrating and leading on MI and data reporting.	██████████████████
NHSD	Salesforce Cloud Services (Satellite Manager Ordering Portal)	Responsible for Salesforce Cloud Services.	██████████
NHSD	Contract Lead	Management of all formal Variations of the Call Off Contract and all other contractual matters.	██████████████

Annex 1 – Processing Personal Data

Schedule 7 - GDPR Information

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

Annex 1 - Processing Personal Data

This Annex shall be completed by the Buyer, who may take account of the view of the Subprocessor, 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 Subprocessor shall Process Personal Data on the written instructions of the Processor only and shall comply with any further written instructions with respect to Processing by the Processor.
- 1.4 The written instructions for such Processing are set out in this Annex 1, and are supplemented by the further written instructions set out in the operational document called the 'Description of Processing Activities (the 'DPA')'. The DPA applicable to the Services as at the date of signature of this Call-Off Contract is embedded below:
- [REDACTED]
- 1.5 The Parties agree that any amendments to the DPA shall be approved by a member of the Processor's information governance team or their authorised delegate (escalated to the Department for Health and Social Care as appropriate) and [REDACTED] or his authorised delegate.
- 1.6 The DPA, including any amendments as approved and documented by the Parties in accordance with paragraph 1.5 above, shall be incorporated by reference into this Annex 1.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Department of Health and Social Care is Controller. The Buyer is Processor and the Supplier is Subprocessor</p> <p>The Parties acknowledge that in relation to paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, references to the Controller shall be interpreted as references to the Buyer as Processor, and references to Processor shall be interpreted as references to the Supplier and Subprocessor. The Buyer is the Processor and the Supplier is the Subprocessor of the Personal Data set out in this Schedule 7 (GDPR Information).</p>

Duration of the Processing	In line with instructions received from the Data Processor for the duration of the Call-Off Contract Term, unless instructed to suspend and / or permanently cease the Processing by the Processor.
Nature and purposes of the Processing	<p>The purpose of the Processing is to provide the Services as further described in the Order Form.</p> <p>Deloitte will:</p> <p>Process (including sharing with other processors or sub-processors to either DHSC or NHS Digital engaged in the National Testing Service, e.g. [REDACTED]) personal data:</p> <ul style="list-style-type: none"> - to facilitate linkage of test results and registration data (e.g. [REDACTED]) - to calculate age of sample, and determine if it is stable enough to process, or if it requires prioritisation (e.g. [REDACTED]) - to facilitate the ordering and delivery of Home Test kits (e.g. [REDACTED]) - to enable booking for RTS/LTS/MTU testing, (e.g. [REDACTED]) - to provide Management Information capabilities (MI) - within mobile applications used in the operational testing process (e.g. to register vehicles, to track test samples, etc) - to assist NHS Digital in analysing data and investigating/monitoring service/performance issues - to enable individuals to receive notification of their test results. <p>Supply registration data to NHS Wales in order for Welsh testing to be administered.</p> <p>Supply contact details to the Contract Tracing System (currently CTAS, operated by PHE).</p> <p>Operate an Admin Portal, which is used by call centre agents and staff from other organisations (other processors or sub-processors to either DHSC or NHS Digital engaged in the National Testing Service, or to</p>

	<p>DHSC or NHS Digital, e.g. NHS Digital service integration team and South-Central Ambulance Service (SCAS)). This Admin Portal provides:</p> <ul style="list-style-type: none"> - 1. 119 Assisted Registration Channel - 2. Barcode Lookup feature – predominantly used by 119 but also various service desks and to solve SCAS complaints - 3. “Bulk SMS” tool to distribute SMS messages en masse to people booked for test site appointments that are disrupted - 4. “Super user” creator tool for to make organisations and super users for Elective Care NHS Trusts - 5. Channel manager to make different test site and home testing channels available or not (for digital self service) - 6. Study creator and management tool for service evaluations <p>Share personal data with third party organisations where instructed to do so by either NHS Digital or DHSC.</p>
Type of Personal Data	<p>The types of Personal Data being Processed include:</p> <p>Identifying details of individuals. This includes items which identify individuals, as well as contact details and demographic detail. Examples include: Names, addresses, dates of birth, gender, ethnicity, NHS numbers, telephone numbers, email addresses and vehicle registration numbers.</p> <p>Health information of individuals. This includes the details and results of COVID-19 tests, reported symptoms, immunity status and underlying health conditions.</p> <p>Employment information of individuals. This includes occupation, employer and industry of employment.</p>
Categories of Data Subject	<ul style="list-style-type: none"> • Key workers and family members of key workers • Members of the general public • Care Home residents and staff • Staff and inmates in the secure and detained estate (e.g. prisons)
<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>At the written direction of the Processor, securely delete or securely return the Personal Data (and any copies of it) to the Processor promptly following the earlier of:</p> <ul style="list-style-type: none"> a) termination or expiry of this Call-Off Contract; or b) a request from the Processor or unless the Subprocessor is required by Law to retain the Personal Data.

Annex 2 - Joint Controller Agreement – Not applicable

Annex 3 – Data Security

1. Without prejudice to the Subprocessor's other obligations in respect of information security, the Subprocessor shall:
 - 1.1. having regard to the state of technological development, provide a level of security (including appropriate technical and organisational measures) appropriate to:
 - 1.1.1. the harm that might result from unauthorised or unlawful processing of Personal Data or accidental loss, destruction or damage of such Personal Data; and
 - 1.1.2. the nature of the Personal Data;
 - 1.2. take reasonable steps to ensure the reliability of the Processor's Personnel who have access to the Personal Data which shall include:
 - 1.2.1. ensuring all such Processor Personnel understand the confidential nature of the Personal Data and the issues which arise if proper care is not taken in the processing of the Personal Data;
 - 1.2.2. including appropriate confidentiality clauses in employment contracts, including details of sanctions against any employee acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of Data Protection Legislation or causes damage to or loss of Personal Data;
 - 1.2.3. ensuring all such Processor Personnel are properly trained in data protection appropriate to their role, and to ensure that all such Processor Personnel have completed such training prior to their use of the Personal Data. Where requested to do so the Subprocessor shall provide examples of training materials used, together with methodologies used to demonstrate that Processor Personnel have understood the training. Training shall be repeated at regular intervals to take account of developments in law on good data protection practice and in any event on an annual basis;
 - 1.2.4. ensuring all such Processor Personnel are properly vetted, both during the initial recruitment process and throughout their engagement in their processing of the Personal Data, including through the use of procedures to identify changes in personal circumstances which may affect an individual's ability to process the Personal Data in accordance with the terms of this Call-Off Contract;
 - 1.2.5. ensuring only those Processor Personnel involved in the delivery of the Data Processing have access to the Personal Data and implementing appropriate access controls to ensure this requirement is satisfied;
 - 1.2.6. provide the Processor with such information, assistance and co-operation as the Processor may require from time to time to establish either Party's compliance with the Data Protection Legislation; and

- 1.2.7. inform the Processor as soon as reasonably practicable of any particular risk to the security of the Personal Data of which it becomes aware, and of the categories of Personal Data and individuals which may be affected.
- 1.3. The Subprocessor shall promptly, and in any event not later than reasonably required in order to enable the Processor to fulfil its duties under the Data Protection Legislation provide such information as the Processor requires relating to the identity of any third parties to whom the Personal Data has been disclosed by the Subprocessor to the extent the Processor requires this information to comply with its duties under the Data Protection Legislation.
- 1.4. The Subprocessor shall ensure:
 - 1.4.1. that it has properly configured access rights for its Processor Personnel including a well-defined joiners and leavers process to ensure access rights to the Personal Data are properly managed;
 - 1.4.2. that it has proper controls in place to make sure that complex alphanumeric passwords are required for access to the Personal Data and that training is provided in relation to the need to keep such passwords secure;
 - 1.4.3. it has in place procedures to identify wrongful use of Personal Data, including the monitoring of wrongful access to Personal Data;
 - 1.4.4. that suitable and effective authentication processes are established and used to protect Personal Data;
 - 1.4.5. that Personal Data is backed up on a regular basis and that all back up data is subject to such vigorous security procedures as are necessary in order to protect data integrity, such security measures being commensurate to the nature of the data, and that a robust business continuity plan is in place. The Subprocessor shall take particular care when transporting backup data and other personal information and shall ensure such backup data and other personal information is transported in a safe and secure manner;
 - 1.4.6. that Personal Data transferred electronically is encrypted using only the Advanced Encryption Standard (AES) – 256 bits specification;
 - 1.4.7. that Personal Data will not be stored on laptops or other portable media unless agreed in writing with the Processor and subject to the following provisions:
 - 1.4.7.1. Personal Data stored on laptops or other portable media is encrypted to at least Advanced Encryption Standard (AES) 256 bits specification and that the Subprocessor maintains an accurate, up to date asset register, including all such portable media used to process the Personal Data;
 - 1.4.7.2. all portable media used for storage or transit of Personal Data are fully encrypted in accordance with the NCSC 10 Steps to Cyber Security and must

meet the standard published by NCSC “Software Encryption of Removable Media: CPA SC”;

1.4.7.3. portable media are not left unattended at any time (e.g. in parked cars, in unlocked & unoccupied rooms, etc.); and

1.4.7.4. when not in use all portable media are stored in a locked area and issued only when required to authorised employees, with a record kept of issue and return.

1.4.8. that Processor Personnel are not able to access the Personal Data from home or via their own electronic device other than through a secure electronic network and that Personal Data may not be stored in such devices;

1.4.9. that suitable physical security measures are established commensurate to the harm that could result from the unlawful disclosure of and/or access to the Personal Data. Such physical security measures shall be as identified in the Subprocessor’s data protection policy;

1.4.10. that suitable physical security measures are established to ensure that the Personal Data is protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood;

1.4.11. without prejudice to the Subprocessor's obligations to NHS Digital in relation to the disposal of Personal Data, all Personal Data which is disposed of must be disposed of in accordance with applicable law and Data Guidance; and

1.4.12. that the Subprocessor establishes and maintains adequate data security compliance policies and audits its use of Personal Data in compliance with its data security policies on a regular basis and in any event annually.

1.5. The Subprocessor shall from the Start Date and throughout the term, remain registered with the DSP Toolkit or any replacement to such system (<https://www.dsptoolkit.nhs.uk>).

Order Form Schedule 2 - Call-Off Contract Charges

Section 1: Resource Charges

Charges until 30 September 2020:

Charges applicable from 1 October 2020:

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Section 2 – Managed Service

Section 3 – Third Party Pass Through

Annex 1 (Third Party Services) to this Section 3 (Third Party Pass Through) sets out the infrastructure and third party elements of the Solution, together with details of the party responsible for procuring the contracts.

Supplier Responsibility:

The Supplier shall pass on the charges at cost of the third-party services designated in Annex 1 (Third Party Services) as “Deloitte responsibility” to the Buyer, provided that the Supplier provides copies of all relevant third-party service invoices in advance to the Buyer.

The Supplier will use the toolsets set out in Annex 1 (Third Party Services) under the “Deloitte responsibility” tab for management of the software development process and will administer the cloud infrastructure for both non-production and production environments, used to deploy and host the web portal and applications.

Buyer Responsibility:

The Supplier is dependent on the third parties set out in Annex 1 (Third Party Services) under the “NHSD responsibility” tab, who will be contracted directly by the Buyer, or may already be contracted or provisioned through an NHS, DHSC or other Government body. The Buyer is responsible for ensuring that these parties and their infrastructure, solutions and services are provisioned for delivery of the functional and technical scope outlined in Order Form Schedule 1. This includes ensuring that the third parties are compliant with relevant security and data obligations.

The third-party applications, software and services described in this Order Form Schedule 1 shall constitute Third Party Software as defined in the Supplier Terms incorporated in the Call Off Contract.

Annex 1 – Third Party Services

Tool	Description	Contract/T&Cs/Terms of Service	Licence Owner	Invoice Dates
Atlassian (Confluence, JIRA, Zephr for JIRA, Draw.IO)		https://www.atlassian.com/legal/software-license-agreement	Deloitte	Monthly (27th)
Zeplin		https://zeplin.io/terms	Deloitte	Monthly (27th)
Abstract		https://www.abstract.com/legal/customer-terms-of-service	Deloitte	annual licences (29/04/20 - 29/04/21) annual licences (01/06/20 - 29/04/21)
AWS (P000296) - AMS Core Application		https://aws.amazon.com/service-terms/	Deloitte	
AWS (P000297) - Amazon Connect Implementation (Service Desk)		https://aws.amazon.com/service-terms/	Deloitte	
AWS (P000293) - Employer Referral Portal		https://aws.amazon.com/service-terms/	Deloitte	
AWS (P000304) - MI Solution		https://aws.amazon.com/service-terms/	Deloitte	
Azure DevOps		https://azure.microsoft.com/en-gb/support/legal/	Deloitte	
SonarQube		https://www.sonarqube.org/docs/Sonarsource-SAs-Terms-and-Conditions-for-the-use-of-the-SONARQUBE-brand.pdf	Deloitte	Annually (28/05/20 - 27/05/21)
RapidSpike		https://www.rapidspike.com/info/terms-conditions/	Deloitte	Monthly (29th)
Xcode develop		https://www.apple.com/legal/sla/docs/xcode.pdf	Deloitte	
BrowserStack - Automate Mobile		https://www.browserstack.com/terms	Deloitte	Monthly (30th)
BrowserStack - Live		https://www.browserstack.com/terms	Deloitte	Monthly (2nd)
Scandit (Barcode Scanner SDK Native)		https://ssl.scandit.com/terms/test.pdf https://ssl.scandit.com/terms/community.pdf	Deloitte	Quarterly (starting 13/07/20)
Scandit (Barcode Scanner SDK for Web)		https://ssl.scandit.com/terms/test.pdf https://ssl.scandit.com/terms/community.pdf	Deloitte	Annually (13/04/20 - 13/04/21)
Realm		https://realm.io/legal/	Deloitte	N/A
RealmSwift		https://realm.io/legal/	Deloitte	N/A
SwiftLint		https://realm.github.io/SwiftLint/rule-directory.html	Deloitte	N/A
ManagedAppConfigLib		https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy	Deloitte	N/A
AppAuth			Deloitte	N/A
ReachabilitySwift			Deloitte	N/A
Embassy			Deloitte	N/A
EnvoyAmbassador			Deloitte	N/A
Micro Focus Fortify		https://www.microfocus.com/en-us/legal/software-licensing	Deloitte	Annually
Snyk		https://snyk.io/policies/terms-of-service/	Deloitte	Annually (16/07/20 - 16/07/21)

Arcsight		https://www.microfocus.com/en-us/legal/end-user-agreement/terms	Deloitte	N/A	
PagerDuty		https://www.pagerduty.com/terms-of-service/	Deloitte		
ServiceNow		https://www.servicenow.com/content/dam/servicenow/assets/public/en-us/docs/type/legal/servicenow-general-terms-and-conditions.pdf	Deloitte		
OutSystems		https://www.outsystems.com/legal/master-subscription-agreement/	Deloitte		
UIPath		https://www.uipath.com/developers/all-editions/license-agreement	Deloitte		

Area	Third party	
[REDACTED]	Jigsaw24 devices	[REDACTED]
	Jigsaw24 service desk	[REDACTED]
	Vodafone	[REDACTED]
[REDACTED]	Barcoding	[REDACTED]
[REDACTED]	ACF	[REDACTED]
[REDACTED]	GDS Gov.notify delivery service	[REDACTED]
	GDS Gov.uk domains	[REDACTED]
	Mesh data transfer from NHS (NPEx)	[REDACTED]
	Tableau	[REDACTED]
	Salesforce licenses	[REDACTED]
[REDACTED]	Salesforce - mailbox hosting	[REDACTED]
[REDACTED]	Salesforce - teleperformance	[REDACTED]

Part B – Terms and Conditions

1. Call-Off Contract start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)

- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary Supplier Staff vetting as specified by the Buyer

- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

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

6. Business continuity and disaster recovery

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

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
- during this Call-Off Contract, Subcontractors hold third-party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
 - the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
 - all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
 - all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
- a broker's verification of insurance
 - receipts for the insurance premium
 - evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
 - promptly notify the insurers in writing of any relevant material fact under any insurances
 - hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

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

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

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

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

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

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

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

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

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

13. Buyer data

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

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

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

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

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its

corruption and loss.

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

- the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/collection/risk-management-collection>
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

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

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

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

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

14. Standards and quality

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

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

- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

16. Security

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

Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.

- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

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

18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.
- 18.2 The Parties agree that the:
- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
 - Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses
- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

- any fraud

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

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

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

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

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

20. Notices

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

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

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

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
 - there will be no adverse impact on service continuity
 - there is no vendor lock-in to the Supplier's Service at exit
 - it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
 - the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
 - the testing and assurance strategy for exported Buyer Data
 - if relevant, TUPE-related activity to comply with the TUPE regulations
 - any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

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

23. Force majeure

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

24. Liability

- 24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:
- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
 - Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
 - Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes

to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

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

26. Equipment

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

30. Additional G-Cloud services

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

31. Collaboration

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

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-

Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

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

33. Data Protection Legislation (GDPR)

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

Schedule 3 - Collaboration agreement

This agreement is made on [enter date]

between:

- 1) [Buyer name] of [Buyer address] (the Buyer)
- 2) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
- 3) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
- 4) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
- 5) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
- 6) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

- Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
- Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

- “Agreement” means this collaboration agreement, containing the Clauses and Schedules
- “Call-Off Contract” means each contract that is let by the Buyer to one of the Collaboration Suppliers
- “Contractor’s Confidential Information” has the meaning set out in the Call-Off Contracts
- “Confidential Information” means the Buyer Confidential Information or any Collaboration Supplier’s Confidential Information
- “Collaboration Activities” means the activities set out in this Agreement
- “Buyer Confidential Information” has the meaning set out in the Call-Off Contract

- “Default” means any breach of the obligations of any Collaboration Supplier or any default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties
- “Detailed Collaboration Plan” has the meaning given in clause 3.2
- “Dispute Resolution Process” means the process described in clause 9
- “Effective Date” means [insert date]
- “Force Majeure Event” has the meaning given in clause 11.1.1
- “Mediator” has the meaning given to it in clause 9.3.1
- “Outline Collaboration Plan” has the meaning given to it in clause 3.1
- “Term” has the meaning given to it in clause 2.1
- "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the “Term”).

- 2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

- 3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the "Outline Collaboration Plan").
- 3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the "Detailed Collaboration Plan"). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier's respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.
- 3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.
- 3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:
- 3.4.1 approve the Detailed Collaboration Plan
 - 3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection
- 3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.
- 3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

- 4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.
- 4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.
- 4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all co-operation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

- 5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.
- 5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

- 6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.
- 6.2 Each Collaboration Supplier warrants that:
- 6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement
 - 6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party
 - 6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors
 - 6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise
- 6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:
- 6.3.1 or becomes public knowledge other than by breach of this clause 6
 - 6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party
 - 6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure
 - 6.3.4 independently developed without access to the Confidential Information
 - 6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction
- 6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

- 7.1 Each Collaboration Supplier warrant and represent that:
- 7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£ ,000)].

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage

8.5.2 special loss or damage

8.5.3 consequential loss or damage

8.5.4 loss of profits (whether direct or indirect)

8.5.5 loss of turnover (whether direct or indirect)

8.5.6 loss of business opportunities (whether direct or indirect)

8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

- 9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.
- 9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.
- 9.3 The process for mediation and consequential provisions for mediation are:
- 9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the Chairman of the Law Society to appoint a Mediator
 - 9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations
 - 9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings
 - 9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives
 - 9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non-binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties
 - 9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts
- 9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

- 10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing

to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

11.5.1 Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 **Variations**

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 **No waiver**

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 **Governing law and jurisdiction**

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

Collaboration Agreement Schedule 1 - List of contracts

Collaboration supplier	Name/reference of contract	Effective date of contract

--	--	--

[Collaboration Agreement Schedule 2 - Outline collaboration plan]

Schedule 4 - Alternative clauses

1. Introduction

- 1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

- 2.1 The Customer may, in the Order Form, request the following alternative clauses:

2.1.1 Scots Law (see paragraph 2.1.2 of this Schedule)

2.1.2 Scots Law

Law and Jurisdiction

References to England and Wales in incorporated Framework Agreement clause 8.10 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1

Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

References to "tort" will be replaced with "delict" throughout.

- 2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.7.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular, the Employment (Northern Ireland) Order 2002, the Fair Employment and Treatment (Northern Ireland) Order 1998, the Sex Discrimination (Northern Ireland) Order 1976 and 1988, the Employment Equality (Sexual Orientation) Regulations (Northern Ireland)

2003, the Equal Pay Act (Northern Ireland) 1970, the Disability Discrimination Act 1995, the Race Relations (Northern Ireland) Order 1997, the Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996 Employment Equality (Age) Regulations (Northern Ireland) 2006; Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000; Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002, The Disability Discrimination (Northern Ireland) Order 2006, The Employment Relations (Northern Ireland) Order 2004, The Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006, The Employment Relations (Northern Ireland) Order 2004 and The Work and Families (Northern Ireland) Order 2006; and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

- a. persons of different religious beliefs or political opinions
- b. men and women or married and unmarried persons
- c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- f. persons of different ages
- g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- a. the issue of written instructions to staff and other relevant persons
- b. the appointment or designation of a senior manager with responsibility for equal opportunities

- c. training of all staff and other relevant persons in equal opportunities and harassment matters
- d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

- a. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- b. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or Court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

- 2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.
- 2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.
- 2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.
- 2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.
- 2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

- 2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).
- 2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.
- 2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.
- 2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5 - Guarantee

[A Guarantee should only be requested if the Supplier's financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary's requirements]

This deed of guarantee is made on [insert date date/month/year] between:

- (1) [Insert the name of the Guarantor] a company incorporated in England and Wales with number [insert company number] whose registered office is at [insert details of the guarantor's registered office] [or a company incorporated under the Laws of [insert country], registered in [insert country] with number [insert number] at [insert place of registration], whose principal office is at [insert office details]] ('Guarantor'); in favour of

and

- (2) The Buyer whose offices are [insert Buyer's official address] ('Beneficiary')

Whereas:

- (A) The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.
- (B) It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn't needed then the section below and other references to the guarantee should be deleted.]

Suggested headings are as follows:

Demands and notices

Representations and Warranties

Obligation to enter into a new Contract

Assignment

Third Party Rights

Governing Law

This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.]

Guarantor company	[Company name] 'Guarantor'
Guarantor company address	[Company address]
Account	Name: [Account Manager name]

manager:	Address: [Account Manager address]
	Phone: [Account Manager phone]
	Email: [Account Manager email]
	Fax: [Account Manager fax (if applicable)]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	Meaning
Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].
Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.

Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words 'other' and 'otherwise' are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

- reference to a gender includes the other gender and the neuter
- references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time
- any phrase introduced by the words 'including', 'includes', 'in particular', 'for example' or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

- fully perform or buy performance of the guaranteed obligations to the Buyer
- as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[Address of the Guarantor in England and Wales]

[Email address of the Guarantor representative]

For the Attention of [insert details]

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

- delivered by hand, at the time of delivery
- posted, at 10am on the second Working Day after it was put into the post
- sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

- any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
- any amendment to or termination of the Call-Off Contract
- any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
- the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

- it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee
- it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person
- if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor
- the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

- obtain judgment against the Supplier or the Guarantor or any third party in any court
- make or file any claim in a bankruptcy or liquidation of the Supplier or any third party
- take any action against the Supplier or the Guarantor or any third party
- resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer's rights may be exercised as often as the Buyer deems expedient.

Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may

determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

- the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation
- has the capacity to sue or be sued in its own name
- the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets
- the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee
- the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:
 - the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgment, decree or permit to which the Guarantor is subject
 - the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets
 - all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor's acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of Guarantee by any

representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers [the Supplier] [a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [insert fax no.] from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[Insert name of the Guarantor] acting by [Insert names]

Director

Director/Secretary

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

	Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: <ul style="list-style-type: none"> • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: <ul style="list-style-type: none"> i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data

	and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<p>A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare

	<ul style="list-style-type: none"> • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.11 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2 .
Guarantee	The guarantee described in Schedule 5.

Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: <ul style="list-style-type: none"> • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.

Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited Act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the

	Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security Management Plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the

	Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

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

Annex 1 - Processing Personal Data

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

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

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">• [Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer] <p>The Supplier is Controller and the Buyer is Processor</p> <p><i>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:</i></p> <ul style="list-style-type: none">• [Insert the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier] <p>The Parties are Joint Controllers</p> <p><i>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none">• [Insert the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together] <p>The Parties are Independent Controllers of Personal Data</p>

	<p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> <i>Business contact details of Supplier Personnel for which the Supplier is the Controller,</i> <i>Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller,</i> [Insert the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer] <p>[Guidance where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]</p>
Duration of the Processing	[Clearly set out the duration of the Processing including dates]
Nature and purposes of the Processing	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.]</p> <p>The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</p>
Type of Personal Data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]

<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p><i>[Describe how long the data will be retained for, how it be returned or destroyed]</i></p>
--	--

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

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

1.2 The Parties agree that the [Supplier/Buyer]:

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

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

2. Undertakings of Both Parties

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

- (a) report to the other Party every [x] months on:
 - (i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
 - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
 - (iii) any other requests, complaints or communications from Data Subjects (or third parties

on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex.
- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
 - (i) nature of the data to be protected;
 - (i) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

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

3. Data Protection Breach

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

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

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

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

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

4. Audit

4.1 The Supplier shall permit:

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

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

5. Impact Assessments

5.1 The Parties shall:

- (a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

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

- (a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

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

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

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

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any

other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

9. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 18.5 (*Ending the contract*).

10. Sub-Processing

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

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

11. Data Retention

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