



Crown
Commercial
Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Part A: Order Form 2

Principal contact details3

Call-Off Contract terms4

Buyer contractual details5

Supplier’s information9

Call-Off Contract charges and payment 10

Additional Buyer terms 11

1. Formation of contract 20

2. Background to the agreement 20

Schedule 1: Services 21

Schedule 2: Call-Off Contract charges 23

Part B: Terms and Conditions 25

Schedule 3: Collaboration agreement: Not Applicable 44

Schedule 4: Not Applicable Schedule 5: Not Applicable 44

Schedule 6: Glossary and interpretations 44

Schedule 7: GDPR Information 56

Annex 1: Processing Personal Data 56

Annex 2: Joint Controller Agreement 62

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	8668 2373 5523 895
DHSC Call-Off Contract reference	Project Ref: C32762
Call-Off Contract title	National Institute for Health Research (NIHR) Information Systems (IS) Function Contract
Call-Off Contract description	Corporate NIHR IS Services including hosting and provision of email, shared hosting and storage, collaborative tools and help desk support to 8,000 NIHR researchers, research bodies, staff, students across the United Kingdom
Start date	01/09/2021
Expiry date	31/08/2023
Call-Off Contract value	<p>Price Per Annum = £2,927,200.00</p> <p>Cumulative costs:</p> <ul style="list-style-type: none"> • Year 1 Cost: £2,927,200.00 • Year 2 Cost: £5,854,400.00 • Year 3 Cost (subject to approvals & agreement of extension): £8,781,600.00 • Year 4 Cost (subject to approvals & agreement of extension): £11,708,800.00
Charging method	Fixed Price and other, usage-based charges – see Schedule 2
Purchase order number	TBC

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

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

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

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

From the Buyer	The Secretary of State for Health and Social Care acting as part of the Crown through the Department of Health and Social Care Department of Health and Social Care, Science Research and Evidence Directorate [REDACTED] Victoria Street London SW1H 0EU
To the Supplier	PA Consulting Services Ltd [REDACTED] 10 Bressenden Place London SW1E 5DN Company number: 414220
Together the 'Parties'	

Principal contact details

For the Buyer:	For the Supplier:
Deputy Director, Research Systems [REDACTED] Email: [REDACTED] Phone: [REDACTED]	Member of PA Consulting's Management Group [REDACTED] Email: [REDACTED] Phone: [REDACTED]

Call-Off Contract terms

Start date	This Call-Off Contract Starts on 01/09/2021 and is valid for an initial term of 24 months with the possibility of 1 year extension and another 1 year extension
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 90 days from the date of written notice for Ending without cause (as per clause 18.1).</p>
Extension period	<p>This Call-off Contract can be extended by the Buyer for 2 (two) periods of up to 12 (twelve) months each, by giving the Supplier 8 weeks written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p> <p>The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.</p> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p>https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</p>

Buyer contractual details

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

G-Cloud lot	Lot 3
G-Cloud services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <p>Delivering Service Integration and Managed Service (SIAM)</p>
Additional Services	None.
Location	The Services will be delivered virtually/remotely and to National Institute for Health Research locations and DHSC offices as required
Quality standards	The quality standards required for this Call-Off Contract are as set out in Schedule 1.
Technical standards:	The technical standards required for this Call-Off Contract are as set out in Schedule 1.
Service level agreement:	<p>The service level and availability criteria required for this Call Off Contract are:</p> <p>Service Desk Support: as described in Schedule 1 and in accordance with the applicable service levels available under the relevant Third Party Terms.</p> <p>Scorecard SLA process</p> <p>The Buyer and the Supplier will agree a templated Balanced Scorecard together with a performance management plan, which clearly outlines the responsibilities and actions that will be taken if agreed performance levels are not achieved.</p>
Onboarding	Not Applicable

Offboarding	<p>The offboarding plan for this Call-Off Contract is to be defined by the Supplier within the first three months following the start date of 1 September 2021 in an “Exit Management Plan”, and will include;</p> <ul style="list-style-type: none">• a schedule of payments (all exit services will be subject to the Supplier’s rate card)• Provision of an Exit Manager who will be appointed for the purposes of managing the Supplier’s obligations under this schedule and the Department of Health and Social Care will be informed of this appointment.• Using reasonable endeavours to maintain its existing management team during the period of any exit assistance services.• A register of all Third Party Components that make up the NIHR hub including Google Workspace including 16 cloud based applications, the NIHR website, Helpdesk Service• Supplier to provide training and support with replacement supplier• All documentation relating to the management of the NIHR IS function including all administrative passwords• Supplier to provide any other information or assistance reasonably required by the Department of Health and Social Care or a Replacement Supplier in order to affect an orderly handover of the provision of the Services.
Collaboration agreement	Not applicable

Limit on Parties' liability	<p>The annual total liability of either Party for all Property Defaults will not exceed 125%.</p> <p>The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none">• a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract• professional indemnity insurance cover to be held by the Supplier. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim (and as required by Law).• employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.
Force majeure	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 40 consecutive days.</p>

Audit	<p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable PA Consulting Ltd to carry out audits</p> <p>DHSC acknowledges that the Supplier's IT Systems, payroll data, non-rechargeable expenses, overheads or profit and loss information are excluded from the scope of the audit carried out on behalf of DHSC</p>
Buyer's responsibilities	<p>The Buyer is responsible for acting as customer for the NIHR IS Function</p> <p>The Buyer shall co-operate with the Supplier in any manner is reasonably necessary</p> <p>The Buyer will comply with the applicable Third Party Terms associated with the Third Party Components listed in the section below (Subcontractors or partners / Third Party Components).</p> <p>The Buyer will provide information and data and make available its personnel as reasonably required for the Supplier to deliver the Services.</p>
Buyer's equipment	N/A.

Supplier’s information

Subcontractors or partners	The following is a list of the Supplier’s Subcontractors or Partners	
	PA Holdings Limited and the following vendors of the Third Party Components that make up the NIHR Hub:	
Third Party Components	Company	Third Party Component
	[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]

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is BACS .
Payment profile	The payment profile for this Call-Off Contract is monthly in arrears.
Invoice details	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Invoices should in the first instance be sent to: [REDACTED] or another DHSC SRE official if notified by DHSC SRE Colleagues, for processing and payment. The contractor may also send copies to [REDACTED] Accounts Payable - Department of Health & Social Care for information only.
Invoice information required	All invoices must include a valid purchase order number.
Invoice frequency	Invoice will be sent to the Buyer monthly in arrears.
Call-Off Contract value	The total value of this Call-Off Contract is £5,854,400.00 (as described in Schedule 2) in line with a 2 year contract, although value may change subject to extension if extension options built into this contract are taken up
Call-Off Contract charges	The breakdown of the Charges is set out in Schedule 2.

Additional Buyer terms

Guarantee	N/A.
Warranties, representations	N/A.
Supplemental requirements in addition to the Call-Off terms	N/A.
Alternative clauses	N/A.
Buyer specific amendments to/refinements of the Call-Off Contract terms	<ol style="list-style-type: none"> 1. Paragraph 4 of the Supplier Terms governs the supply of the Third Party Components referred to in this Order Form 2. The applicable Third Party Terms have been notified to the Buyer and will be incorporated into this agreement. To the extent there are any changes, these will be recorded in the register of Third Party Components prepared in conjunction with the Exit Management Plan. 3. Record Within the scope of the Call-Off Contract, the Supplier is permitted to retain, during and after expiry or termination of the Call-Off Contract, copies of the Buyer's Confidential Information and Buyer Data (but not personal data) stored on the Supplier's back-up and archive media created in the ordinary course of the Supplier's business as part of the Supplier's professional record keeping and business continuity practices. Any such retained copies of the Buyer's Confidential Information and Buyer Data shall: (a) stored in a way so that they are not generally

	<p>accessible by the Supplier's Staff, remain subject to the Supplier's obligations of confidentiality (as set out in clause 8.83 to 8.91 of the Framework Agreement incorporated into the Call-Off Contract by Clause 2.1) and security (as set out in Clause 13 of the Call-Off Contract).</p> <p>4. Third Party Software</p> <p>a. The Buyer has requested that the Services include Third Party Products selected by the Buyer. Third Party Products are the products, software, platforms and infrastructure listed in the table below or later agreed to by the Parties (which may be over email between [Mark Toal or delegate] for the Buyer and James Mucklow for the Supplier, or such other persons as they may designate from time to time).</p> <p>b. The Buyer acknowledges that vendors of the Third Party Products do not generally negotiate the terms of service (TOS) applying to their Third Party Products. In order for the Supplier to comply with the TOS for the various Third Party Products and to ensure that this Call-Off Contract is consistent with the relevant TOS, the Parties agree to the following amendments and refinements to the Call-Off Contract terms:</p>
--	--

- | | |
|--|---|
| | <ul style="list-style-type: none">c. Clause 11.3 does not apply to third-party IPRs in the Third Party Products. The Buyer must not publish (including as open source) the third-party IPRs in the Third Party Productsd. For the purposes of Clause 11.4, the Buyer approves the TOS applying to the Third Party Products listed below.e. The Buyer must comply with the relevant TOS and ensure that its end users also comply. The TOS consists of the Specific TOS for the relevant Third Party Products listed below (or later agreed to by the Parties) and the General TOS listed below (which applies to all Third Party Products). If there is a conflict between the General TOS and the Specific TOS particular Third Party Products, the Specific TOS shall prevail.f. The Supplier will not be considered to be in breach of or liable under this Call-Off Contract if the breach or liability is caused by any of the Third Party Products and the breach or liability occurred despite the Supplier exercising a reasonable degree of care and foresight to endeavour to avoid the breach or liability. |
|--|---|

- g. Notwithstanding c) above, if the Supplier is found liable under this Call-Off Contract and that liability has been caused by any of the Third Party Products, the Parties agree that the amount of the Supplier's yearly total liability (as referred to in Clause 24.1 and in this Order Form) shall be reduced to the amount that the Supplier can recover from the vendors of the Third Party Services less the Supplier's costs of recovery.

General TOS applying to all Third Party Products:

Rights of Use

1. The Supplier grants the Buyer a non-exclusive, non-transferable right, without the right to grant sub-licences, to use and to permit the authorised users to use the Third Party Products during the term of the Call-Off Contract, solely for the Buyer's internal business operations. The Buyer acknowledges and agrees that the Supplier's licensors own all intellectual property rights in the Third Party Products and they do not constitute Project Specific IPRs or Background IPRs. Except as expressly stated in these General TOS or in the Specific TOS, this Call-Off Contract does not grant Buyer any rights to, third-party IPRs in respect of Third Party Products.

	<p>2. The Supplier will maintain a service catalogue defining the number of authorised users able to use the Third Party Products and any other usage limitations in line with the agreements with the vendors of the Third Party Products.</p> <p>Usage Restrictions</p> <p>3. The Buyer shall not access, store, distribute or transmit any Malicious Software or any material during its use of the Third Party Products that is:</p> <ul style="list-style-type: none">a. unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensiveb. facilitates illegal activity;c. depicts sexually explicit images;d. promotes unlawful violence;e. discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; orf. otherwise illegal or causes damage or injury to any person or property; and Supplier reserves the right, without liability, to disable the Buyer's access to any material that breaches the provisions in this paragraph
--	---

4. The Buyer must not, except as may be allowed by any applicable law which is incapable of exclusion by agreement between the Parties:

- a. attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the software and/or documentation made available to the Buyer through the Third Party Products (as applicable) in any form or media or by any means; or
- b. attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the software made available to Buyer through the Third Party Products; or
- c. access all or any part of the Third Party Products in order to build a product or service which competes with the Third Party Products; or
- d. use the Third Party Products to provide services to third parties; or
- e. license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Third Party Products available to any third party except the authorised users, or

- f. attempt to obtain, or assist third parties in obtaining, access to the Third Party Products otherwise than as permitted in this paragraph.

5. The Buyer must prevent any unauthorised access to, or use of, the Third Party Products and, in the event of any such unauthorised access or use, promptly notify the Supplier.

6. The Supplier may suspend the Buyer's access to Third Party Products if the Buyer does not comply with these General TOS or the Specific TOS applying to the Third Party Products.

Availability

7. The Supplier will use commercially reasonable endeavours to make the Third Party Products available during Normal Business Hours, subject to the service levels applying to the Third Party Products and outages during maintenance. Supplier will use reasonable endeavours give Buyer advance notice of maintenance. Normal Business Hours are from 8am to 6pm on a day (other than a Saturday, Sunday or public holiday) when banks in London are open for business.

8. Notwithstanding anything to the contrary in the Call-Off Contract, the Supplier:

- a. does not warrant that the availability of the Third Party Products will exceed the availability or service levels provided to the Supplier by the vendors of the Third Party Products;

- b. does not warrant that the Buyer's use of the Third Party Products will be uninterrupted or error-free;
 - c. is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Buyer acknowledges that the Third Party Products may be subject to limitations, delays and other problems inherent in the use of such communications facilities.
9. The Supplier may, without liability but with reasonable notice, disable the Buyer's access to Third Party Products if the Supplier is required to do so by a vendor of the Third Party Products.
10. If all or part of the Third Party Products are not available, the Supplier will inform the Buyer and the Parties shall discuss and agree work-arounds and, if necessary, replacement products

	<p>Loss of Buyer Data caused by Third Party Products</p> <p>11. Notwithstanding anything to the contrary in the Call-Off Contract, the Supplier is not responsible for any loss, destruction, alteration or disclosure of Buyer Data caused by any vendor of Third Party Products (except those third parties sub-contracted by the Supplier to perform services related to Buyer Data maintenance and back-up) caused by Malicious Software originating from the Third Party Products.</p> <p>Buyer Personal Data</p> <p>12. The Buyer is responsible for obtaining and maintaining any consents required from the data subjects of the Buyer Personal Data required by Data Protection Legislation to allow the Supplier to perform its obligations under the Call-Off Contract and provide the Third Party Products. The Supplier will provide the Buyer with all reasonable assistance in obtaining and maintaining such consents.</p> <p>13. The Buyer's use of the Third Party Products may involve the transfer or storage of Buyer Personal Data to locations outside of the European Union or the country where the Buyer and the data subjects are located. The Supplier will provide the Buyer with all reasonable assistance to ensure that such transfers of Buyer Personal Data are in accordance with Data Protection Legislation.</p>
--	---

Public Services Network (PSN)	N/A
GDPR	In line with Annex 1 Annex 2 and NIHR GDPR Policy

1. Formation of contract

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

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	DHSC
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	12-Jul-2021 6:43 AM EDT	12-Jul-2021 4:13 PM CEST

Schedule 1: Services

Service and Integration Management (SIAM)

The services below are required to be in place from the commencement of the contract and be delivered with no break in continuity. It is anticipated that the Supplier will operate on a monthly fee basis for the provision of the Services utilising a fixed fee where possible. It is also expected that the Supplier will operate in line with Government policy on IT including “Cloud First” and any other applicable policies or future policies.

DHSC would expect continuity of these services between contracts and suppliers.

The priority high level requirements and outcomes for the NIHR IS Function from September 2021 have been identified as follows and are deemed as ‘essential services’; should there be any change in service provision:

- Management and Development of the NIHR Hub, ensuring it reflects the latest Google changes and developments to Google Workspace (or any subsequent service developed) and other Google applications. This includes Business as Usual activities (including, maintenance, delivery and development of the NIHR Hub central corporate functions, systems and services, ensuring value for money at all times;
 - The NIHR Hub based primarily around Google Workspace and a number of 3rd Party applications which provide additional functionality and security of NIHR Hub users.
 - Currently the Hub has:
 - approximately 7.3k users
 - using 9.5Tb of storage for user files and 1.55Tb of shared files
 - operates Google Meet with 13,328 meetings in last 30 days with an average duration of 35 minutes.
 - sent or received 1.1 million emails over the last 3 days
- Provide training and support for upgrades to services already provided and for new applications as and when necessary;
- Maintenance and Development of NIHR network of “change champions” which are in place to support and develop the roll out of the NIHR Hub to eligible users and to support the IS Function with the delivery of its role;
- Annual licensing arrangements with Google are required to be managed within the ongoing contract with Google which expires in December and will be subject to review. The Supplier will be expected to monitor the service for administration and development purposes as well as providing regular reports back to the Authority of usage
- Annual licensing arrangements with other services that are complimentary or ancillary to the provision of the NIHR Hub. The supplier will be expected to monitor the service for administration and development purposes as well as providing regular reports back to the Authority of usage.
- Maintenance, development and support of the NIHR Website

- Supplier to work with NIHR Content Management System provider to ensure website is available in accordance with the mutually agreed performance management plan. The Supplier shall use commercially reasonable endeavours to ensure:
 - that any scheduled CMS updates are fit for the purpose specified in this Call-Off Contract and do not interfere with the day to day operation of the site; that any updates to hosting service(s) are planned not to disrupt day to day operation;
 - all hosting is patched and maintained in line with supplier recommendations and within good industry standards;
 - site is subject to regular (at least annual) penetration and other security testing and
 - any defects resolved within the timescales set out in the performance management plan;
 - the site can be rolled back to last known good configuration in the event of significant disruption;
 - the site is monitored against traffic and load usage and modified / balanced / scaled accordingly, subject always to the service levels available from the vendors of the relevant Third Party Components.
- NIHR / PA helpdesk to provide initial support for NIHR website and will triage to Sitekit helpdesk only if appropriate.
- The provision of a helpdesk from 08:00 to 18:00 each working day **at a bare minimum** providing first line support to support users. It must:
 - make use of the extensive knowledge base that has been established.
 - Where necessary support will to be escalated to second line / third party support
 - Provide a self-service ticketing arrangement for the generation and management of help and support has been implemented.
- Provision of a scalable and flexible resource for high value development that support the NIHR IS Function, meet Ministerial priorities and, the development and implementation of the NIHR Digital Strategy. Any new development must be fully compatible with the current NIHR product suite and if necessary, interoperate with other NIHR systems embedded in NIHR business units;
- Provision, maintenance and development of the NIHR's Single Sign On Service – ensuring that multiple systems can be accessed via a single point of entry. This will require working with a number of partner organisations outside of the NIHR who currently, or plan to, utilise the service for external systems;
- Contract management pass through costs and transition from of a small number of knowledge-based services provided as corporate tools to the wider NIHR. These currently include the peer to peer dissemination network; [CHAIN](#) and the registration of NIHR studies onto an internationally recognised clinical trials register [ISRCTN](#) and the associated registration costs; and the

hosting of certain systems on Amazon Web Servers. All these services will be subject to review and are intended to be revised, curtailed or cease during the lifetime of this contract;

- Provision of support to ensure the delivery of the NIHR Digital Strategy and its goals including, but not exclusively, identification, proportionate due diligence, provision and contract management of third-party partners, or any third-party suppliers identified by the DHSC, and pass through costs for these services;
- Provision of quarterly governance and Key Performance Indicators and reviews [to be developed and agreed by the end of December 2021] and a performance dashboard easily accessible to DHSC and the NIHR Digital Office.
- Maintenance of application updates and security patching to all systems and services that fall under the remit of the NIHR IS Function including, but not exclusively the NIHR Hub, the NIHR website and any other hosted services.

Maintain, support and deliver IS Function security for the NIHR including a system penetration exercise to be conducted in consultation and agreement with the DHSC and the NIHR Digital Office on the minimum of an annual basis for the duration of the contract.

Schedule 2: Call-Off Contract charges

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

Service Integration and Management

Price Per Annum = **£2,927,200.00**

Cumulative costs:

Year 1 Cost: £2,927,200.00

Year 2 Cost: £5,854,400.00

Year 3 Cost (subject to approvals & agreement of extension): £8,781,600.00

Year 4 Cost (subject to approvals & agreement of extension): £11,708,800.00

	Year 1 GBP k	Year 2 GBP k	Description
Supplier managed service Fee	[REDACTED]	[REDACTED]	Fixed fee managed service covering operational support. service desk, application support (resolve and manage incidents, problems, requests and changes received for services within IS Function, continuous improvements; managing app updates and security. provision of Service Delivery Manager and NIHR Hub Change Champion - dedicated resource to manage the network and community
Licence	[REDACTED]	[REDACTED]	<p>Management of Google Workspace licensing - used for NIHR platform including:</p> <ul style="list-style-type: none"> * negotiating, agreeing quotes and procuring Google Workspace licenses * Management of licenses - allocating to users, monitoring usage * Google Supplier Management - managing the partnership with Google, including horizon scanning and identifying opportunities for new products <p>Charges are based on number and type of licenses. The proposed charges are based on 4,500 Enterprise RLS (Front-line) licenses and 3,500 Enterprise Plus Licenses</p> <p>Software licences and Software-as-a-Service charges</p>
Development	[REDACTED]	[REDACTED]	<p>10 days per month of development work for small changes is included in the Managed Service fee</p> <p>Other development work will be costed using the G-Cloud rate card</p>
Hosting	[REDACTED]	[REDACTED]	Infrastructure-as-a-Service cloud consumption charges for hosted applications
Other	[REDACTED]	[REDACTED]	Including Contract Management
Total	£2,927.20	£2,927.20	

The Supplier's managed service fee specified above is fixed and all other fees are variable depending on usage and the applicable Third Party Component fees.

In the event additional services are required these would be price in accordance with the service pricing document, which allows a range of pricing mechanisms, including a rate card for the service, included below.

SFIA Level	Daily Rate
1. Follow	[REDACTED]
2. Assist	[REDACTED]
3. Apply	[REDACTED]
4. Enable	[REDACTED]
5. Ensure/Advise	[REDACTED]
6. Initiate/Influence	[REDACTED]
7. Set Strategy/Inspire	[REDACTED]

Customer Benefits

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

[G-Cloud 12 Customer Benefits Record](#)

Part B: Terms and Conditions

1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 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, provided that 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)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection)
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- 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:

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

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'

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

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 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:
 - 4.1.1 be appropriately experienced, qualified and trained to supply the Services
 - 4.1.2 apply all due skill, care and diligence in faithfully performing those duties
 - 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
 - 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
 - 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

- 5.1 Both Parties agree that when entering a Call-Off Contract they:
 - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
 - 5.1.4 have entered 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 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 a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
- 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
 - 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
 - 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
 - 9.2.4 all agents and professional consultants involved in the Services hold employer's liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
 - 9.4.1 a broker's verification of insurance
 - 9.4.2 receipts for the insurance premium
 - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
 - 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
 - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
 - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
 - 9.8.1 premiums, which it will pay promptly
 - 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

- 10.1 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 8.80 to 8.88. 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:
- 11.5.1 rights granted to the Buyer under this Call-Off Contract
 - 11.5.2 Supplier's performance of the Services
 - 11.5.3 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:
- 11.6.1 modify the relevant part of the Services without reducing its functionality or performance
 - 11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
 - 11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.7 Clause 11.5 will not apply if the IPR Claim is from:
- 11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
 - 11.7.3 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:

- 12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data
- 12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- 12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes
- 12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
 - 12.2.1 providing the Buyer with full details of the complaint or request
 - 12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
 - 12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
 - 12.2.4 providing the Buyer with any information requested by the Data Subject
- 12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.
- 13. Buyer data**
 - 13.1 The Supplier must not remove any proprietary notices in the Buyer Data.
 - 13.2 The Supplier will not store or use Buyer Data except if necessary, to fulfil its obligations.
 - 13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
 - 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
 - 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
 - 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
 - 13.6.1 the principles in the Security Policy Framework:
<https://www.gov.uk/government/publications/security-policy-framework> and
the Government Security Classification policy;
<https://www.gov.uk/government/publications/government-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:

<https://www.cpni.gov.uk/content/adopt-risk-management-approach> and

Protection of Sensitive Information and Assets:

<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance:

<https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

15. Open source

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

16. Security

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

- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

- 18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period 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:

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

18.4.2 any fraud

- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
- 18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
 - 18.5.2 an Insolvency Event of the other Party happens
 - 18.5.3 the other Party ceases or threatens to cease to carry overall or any material part of its business
- 18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
- 18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

- 19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.
- 19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.
- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- 19.4.1 any rights, remedies or obligations accrued before its Ending or expiration
 - 19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

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

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

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

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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

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

20. Notices

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 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:
- 21.6.1 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
- 21.6.2 there will be no adverse impact on service continuity
- 21.6.3 there is no vendor lock-in to the Supplier's Service at exit

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

- 23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 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:

- 24.1.1 Property: for all Defaults by either party 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
- 24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form
- 24.1.3 Other Defaults: for all other Defaults by either party, 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:
- 25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises
- 25.5.2 comply with Buyer requirements for the conduct of personnel
- 25.5.3 comply with any health and safety measures implemented by the Buyer

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
 - 29.2.2 age
 - 29.2.3 start date
 - 29.2.4 place of work
 - 29.2.5 notice period
 - 29.2.6 redundancy payment entitlement
 - 29.2.7 salary, benefits and pension entitlements
 - 29.2.8 employment status
 - 29.2.9 identity of employer
 - 29.2.10 working arrangements
 - 29.2.11 outstanding liabilities
 - 29.2.12 sickness absence
 - 29.2.13 copies of all relevant employment contracts and related documents
 - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer
- 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:
- 29.6.1 its failure to comply with the provisions of this clause
 - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

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

30. Additional G-Cloud services

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

31. Collaboration

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

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract 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 8.59 and 8.60 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 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement: Not Applicable

Schedule 4: Not Applicable

Schedule 5: Not Applicable

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 For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.

Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered 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	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <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 to 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 Controller	Has the meaning given to it in the GDPR
Data Loss Event	Means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under the Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of the Contract, including any Personal Data Breach
Data Processor	Has the meaning given to it in the GDPR
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	<p>Data Protection Legislation means:</p> <ul style="list-style-type: none"> (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Protection Officer	has the meaning given to it in the GDPR
Data Subject	Takes the meaning given in the GDPR
Data Subject Access Request	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data

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 the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here:

	https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into <p>any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</p>
Former Supplier	<ul style="list-style-type: none"> • 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 RM1557.12 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	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand <p>a Schedule A1 moratorium</p>
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership • It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
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 <p>committing or attempting or conspiring to commit Fraud</p>
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in 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. The contact details of the Buyer's Data Protection Officer are: [REDACTED]
2. The contact details of the Supplier's personnel responsible for Data Protection matters on this Call-Off Contract are: [REDACTED]
3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
4. Any such further instructions shall be incorporated into this Annex.

5.

Descriptions	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"> • The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor • Grant applicant, employee, successful candidates, unsuccessful candidates, potential customers, industry collaborators, reviewers, researchers, charity collaborators, senior investigators, system administrators, panel reviewers, communication managers and press officers, infrastructure / research directors and managers, NHS employees, public panel members and all those involved in the administration and management of NIHR research awards <p>The Supplier is Controller and the Buyer is Processor</p> <p>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:</p> <ul style="list-style-type: none"> • N/A
Duration of the Processing	This is for the duration of the contract (01/09/2021 – 31/08/23) in addition, including two yearly extensions if applied. (01/09/23 – 31/08/2024 and 01/09/2024 – 31/08/2025) and for the duration of the exit assistance period.

Nature and purposes of the Processing	<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. The purpose might include: employment Processing, statutory obligation, recruitment assessment etc]</p> <p>The processing takes place to assist the National Institute for Health Research (as part of DHSC) to fund health and care research and translate discoveries into practical products, treatments, devices and procedures, involving patients and the public in all our work.</p>
Type of Personal Data	<p>The processing takes place to assist the National Institute for Health Research (as part of DHSC) to fund health and care research and translate discoveries into practical products, treatments, devices and procedures, involving patients and the public in all our work.</p> <p>The NIHR Hub (Corporate IT services) – including email, document storage and sharing and other collaboration and productivity tools including a corporate directory.</p> <p>Data Collected</p> <ul style="list-style-type: none"> • Formal interactions with NIHR –increasingly NIHR will ask researchers for an ORCID identifier as a consistent and universal identifier of a researcher across NIHR, and beyond. • Name, email address and organisational unit. • Some services may optionally ask for additional data such as date of birth in order to fully participate • Additional information including contact details and job title; associations with organisations and institutions and association with various NIHR activities

	<ul style="list-style-type: none"> For funding applicants possibly collect additional sensitive data relating to equality and diversity (such as ethnicity). This is done by a dedicated Equality and Diversity Reporting System and the information is separately and encrypted.
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of any NIHR website or service
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	<p>As set out in the Supplier's Exit Management Plan. Follows the NIHR Data Retention Strategy which is based on and flows from the DHSC Information Management Policy</p> <p>The approach will be revised if and when necessary</p>
	Third Party Terms associated with the Third Party Components may provide further details on data processing activity and are deemed to be incorporated into this annex.

Protection of Personal Data

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor unless otherwise specified in Schedule 21. The only processing that the Processor is authorised to do is listed in Schedule 21 by the Authority and may not be determined by the Processor.
2. The Processor shall notify the Controller immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.
3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Authority, include:
 - a. a systematic description of the envisaged processing operations in relation to the Services and the purpose of the processing an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - b. an assessment of the risks to the rights and freedoms of Data Subjects; and
 - c. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
4. The Processor shall, in relation to any Personal Data processed in connection with its obligations under the Contract:

- a. process that Personal Data only in accordance with Schedule 21, unless the Processor is required to do otherwise by Law. If it is so required, the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- b. ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measure), having taken account of the:
 - i. nature of the data to be protected;
 - ii. harm that might result from a Data Loss Event;
 - iii. state of technological development; and
 - iv. cost of implementing any measures;
- c. ensure that:
 - i. the Processor Personnel do not process Personal Data except in accordance with the Contract (and in particular Schedule 21);
 - ii. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - 1. are aware of and comply with the Processor's duties under this clause;
 - 2. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - 3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
 - 4. have undergone adequate training in the use, care, protection and handling of Personal Data; and
 - iii. not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - iv. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - v. the Data Subject has enforceable rights and effective legal remedies;
 - vi. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

- vii. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
 - d. at the written direction of the Controller, delete or return Personal Data (and any copies of it to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.
- 5. Subject to Clause 28.6.6, the Processor shall notify the Controller immediately if, in relation to the Personal Data processed under this Agreement, it:
 - a. receives a Data Subject Access Request (or purported Data Subject Access Request);
 - b. receives a request to rectify, block or erase any Personal Data
 - c. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - d. receives any communication from the Information Commissioner or any other regulatory authority;
 - e. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - f. becomes aware of a Data Loss Event.
- 6. The Processor's obligation to notify under Clause 28.6.5 shall include the provision of further information to the Controller in phases, as details become available.
- 7. Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance and assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 28.6.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
 - a. the Controller with full details and copies of the complaint, communication or request;
 - b. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
 - c. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - d. assistance as requested by the Controller following any Data Loss Event;
 - e. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- 8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

- a. the Controller determines that the processing is not occasional;
 - b. the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
 - c. the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
10. Each Party shall designate a data protection officer if required by the Data Protection Legislation.
11. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:
 - a. notify the Controller in writing of the intended Sub-Processor and processing;
 - b. obtain the written consent of the Controller;
 - c. enter into a written agreement with the Sub-Processor which give effect to the terms set out in this Clause such that they apply to the Sub-processor; and provide the Controller with such information regarding the Sub-Processor as the Controller may reasonably require.
12. the Processor shall remain fully liable for all acts or omissions of any of its Sub-Processors.
13. The Controller may, at any time on not less than 30 Working Days' notice, revise this Clause by replacing it with any applicable controller to processor standard Clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
14. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

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

Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

- 1.2 The Parties agree that the Department of Health and Social Care
- (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 National Institute of Health Research 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) handle and report these on a case by case basis.
 - (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;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
- (i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

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

3. Data Protection Breach

- 3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:
- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

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

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

7. Liabilities for Data Protection Breach

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

- 7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:
- (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 procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing disputes).
- 7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):
- (a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;
 - (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses; and
 - (c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.
- 7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Not used

9. Termination

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

10. Sub-Processing

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

11. Data Retention

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