



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

### Contents

G-Cloud 11 Call-Off Contract (version 4)	1
<b>Part A - Order Form</b>	<b>3</b>
Principal contact details	4
Call-Off Contract term	5
Buyer contractual details	5
Supplier's information	6
Call-Off Contract charges and payment	6
Additional Buyer terms	7
<b>Schedule 1 - Services</b>	<b>11</b>
<b>Schedule 2 - Call-Off Contract charges</b>	<b>12</b>
<b>Part B - Terms and conditions</b>	<b>13</b>
1. Call-Off Contract start date and length	13
2. Incorporation of terms	13
3. Supply of services	14
4. Supplier staff	14
5. Due diligence	15
6. Business continuity and disaster recovery	15
7. Payment, VAT and Call-Off Contract charges	16
8. Recovery of sums due and right of set-off	17
9. Insurance	17
10. Confidentiality	18
11. Intellectual Property Rights	18
12. Protection of information	19

13. Buyer data..... 20

14. Standards and quality ..... 21

15. Open source ..... 21

16. Security ..... 21

17. Guarantee ..... 22

18. Ending the Call-Off Contract ..... 22

19. Consequences of suspension, ending and expiry ..... 23

20. Notices ..... 25

21. Exit plan ..... 25

22. Handover to replacement supplier ..... 26

23. Force majeure ..... 27

24. Liability ..... 27

25. Premises ..... 27

26. Equipment..... 28

27. The Contracts (Rights of Third Parties) Act 1999..... 28

28. Environmental requirements ..... 28

29. The Employment Regulations (TUPE) ..... 29

30. Additional G-Cloud services ..... 30

31. Collaboration ..... 30

32. Variation process ..... 30

33. Data Protection Legislation (GDPR)..... 31

**Schedules 3 – 5..... 32**

**NOT USED ..... 32**

**Schedule 6 - Glossary and interpretations..... 33**

**Schedule 7 - GDPR Information ..... 40**

**Annex 1 - Processing Personal Data ..... 40**

## Part A - Order Form

<b>Digital Marketplace service ID number:</b>	501000199851013/31 PILOT / TRIAL
<b>Call-Off Contract reference:</b>	AGEMCSU/TRANS/20/872
<b>Call-Off Contract title:</b>	Provision of Palantir Foundry services
<b>Call-Off Contract description:</b>	Provision of data management platform services
<b>Start date:</b>	12 June 2020
<b>Expiry date:</b>	11 October 2020

<b>Call-Off Contract value:</b>	As set out in Schedule 2
<b>Charging method:</b>	Invoice
<b>Purchase order number:</b>	N/A

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

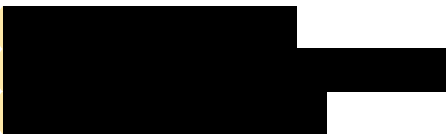
Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

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

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

<b>From: the Buyer</b>	NHS England acting through NHS Arden & GEM CSU (a business unit of National Health Service Commissioning Board of Skipton House, 80 London Road, London, SE1 6LH ( <b>NHS England</b> ))  St Johns House East Street Leicester LE1 6NB
<b>To: the Supplier</b>	Palantir Technologies UK, Ltd. +44 (0) 203 856 8404 Supplier's address: New Penderel House 4th Floor 283 - 288 High Holborn London WC1V 7HP Company number: 07042994
<b>Together: the 'Parties'</b>	

### Principal contact details

<b>For the Buyer:</b>	Title: Chief Data Officer 
-----------------------	--

<b>For the Supplier:</b>	Title: Head of Palantir UK Health [REDACTED]
--------------------------	---

### Call-Off Contract term

<b>Start date:</b>	12 June 2020
<b>Ending (termination):</b>	11 October 2020
<b>Extension period:</b>	Two periods of one month

### Buyer contractual details

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

<b>G-Cloud lot:</b>	Lot 2 - Cloud software Lot 3 - Cloud support
<b>G-Cloud services required:</b>	As set out in Schedule 1. The Supplier acknowledges that the Buyer may permit use of the Service by users within central government departments, agencies and NHS bodies, for the purposes, and as set out in, Schedule 1 and in accordance with this Call-Off Contract, such users to be deemed as Authorised Users under the Licence (as defined below).  The Supplier shall provide support services in relation to the Services in accordance with the "Palantir Service Level Agreement" in effect at the time, which shall for the purposes of this Agreement form part of Schedule 1.
<b>Additional Services:</b>	Not applicable in relation to this Call-Off Contract.
<b>Location:</b>	The Services will be delivered on a remote basis to the Buyer.
<b>Quality standards:</b>	Not applicable
<b>Technical standards:</b>	Not applicable
<b>Service level agreement:</b>	Not applicable
<b>Onboarding:</b>	Not applicable
<b>Offboarding:</b>	Not applicable
<b>Collaboration agreement:</b>	Buyer does not require Supplier to enter into a Collaboration Agreement.
<b>Limit on Parties' liability:</b>	Property (excluding IPR): £50,000 (fifty thousand pounds sterling) in aggregate.  Property (IPR): no limit, on the basis that the Supplier's obligations in clauses 11.5 – 11.8 are replaced by the Supplier's compliance with

	<p>the obligations in clause 11 of the Licence (as defined below) and the Buyer shall observe the obligations of the Customer in that clause 11 in relation to any IPR Claim.</p> <p>Buyer Data: £3 million (five million pounds sterling) in aggregate.</p> <p>Other defaults: 100% of the aggregate Charges payable in the relevant Year.</p>
<b>Insurance:</b>	<p>For the purposes of clause 9, the following additional insurance is required:</p> <p>Cyber liability insurance underwritten by a reputable insurer approved by the Buyer acting reasonably, with a limit of indemnity of at least £10 million pounds sterling each and every claim.</p>
<b>Force majeure:</b>	The number of consecutive days for the purposes of clause 23.1 is 30.
<b>Audit:</b>	<p>The Supplier will maintain the records required by incorporated Framework clause 7.7 during the Term.</p> <p>Clauses 7.6 – 7.11 and 7.13 of the Framework Agreement are incorporated into this Call-Off Contract, provided (a) that an Audit (including security audit referenced below) may be carried out only once during the Term and (b) the Audit may not cover any records held by Buyer or relating to Buyer Data (the parties acknowledging that the Supplier does not have access to Personal Data which identifies Data Subjects as its Processing activity applies only to Personal Data which has been aggregated and de-identified as set out in Schedule 7). (Acknowledging that the Supplier has developed a Security Management Plan and an Information Security Management System meeting the requirements of clause 16) (<b>IS Practice</b>), Supplier will comply with requests for information security audit of the Products from the Buyer and the National Cyber Security Centre (<b>NCSC</b>), and undertakes to notify the Buyer and NCSC of any material changes to IS Practices on request.</p>
<b>Buyer's responsibilities:</b>	As set out in Schedule 1.
<b>Buyer's equipment:</b>	None.

## Supplier's information

<b>Subcontractors or partners:</b>	<p>The following is a list of the Supplier's Subcontractors or Partners:</p> <p>Amazon Web Services (and the Buyer agrees to comply with clause 17 of the Licence in this respect).</p>
------------------------------------	---

## Call-Off Contract charges and payment

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

<b>Payment method:</b>	The payment method for this Call-Off Contract is BACS.
------------------------	--

<b>Payment profile:</b>	The payment profile for this Call-Off Contract is monthly in arrears (if applicable).
<b>Invoice details:</b>	The Supplier will issue electronic invoices monthly in arrears (if applicable). The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
<b>Who and where to send invoices to:</b>	Invoices will be sent to NHS Shared Services, ODE Payables M408, Topcliffe Lane, Phoenix House, Wakefield, WF3 1FE
<b>Invoice information required</b> – for example purchase order, project reference:	All invoices must include a Purchase Order Number.
<b>Invoice frequency:</b>	Invoice will be sent to the Buyer monthly (if applicable).
<b>Call-Off Contract value:</b>	As set out in Schedule 2.
<b>Call-Off Contract charges:</b>	As set out in Schedule 2.

### Additional Buyer terms

<b>Performance of the service and deliverables:</b>	<p>(a) Buyer Data will be hosted in the UK.</p> <p>(b) The Supplier will enable knowledge transfer in accordance with Schedule 1.</p> <p>(c) Further to the provisions of clause 21, the Supplier shall within one month of the Start Date provide the Buyer with an exit plan meeting the requirements of clauses 21.6 and 21.8, including providing Buyer with access to Cloud Content in a format and media reasonably accessible to Buyer for 30 days after the end of the Term.</p> <p>(d) The Supplier shall establish and maintain business continuity and disaster recovery arrangements relating to its operations supporting Service performance in accordance with Good Industry Practice and complying with clauses 6 and 13, and provide a copy to the Buyer for review on request.</p> <p>(e) The Supplier's rights to access and use Buyer Data are only those set out in this Call-Off Contract and the Supplier is not permitted to collect, perform or retain any inspection, analysis, aggregation, evaluation, reproduction, metrics or analytics of Buyer Data or use Buyer Data or any information derived from it as the basis for any product or service, but the Supplier is permitted to collect metrics relating to (a) Buyer's use of Services for the provision of Services including for purposes relating to the information security of the Services and (b) (provided such data is not personally identifiable) usage and diagnostics data for the purposes of analysis, maintenance and improvement of Supplier's products and services, such data related only to the performance, management and efficiency metrics of Products</p>
---	---

	and not including any data accessed or derived from Cloud Content or Buyer Data.
<b>Guarantee:</b>	Not applicable.
<b>Warranties, representations:</b>	<p>The following warranties under incorporated Framework clause 4.1:</p> <ul style="list-style-type: none"> <li>• Supplier Staff with access to Buyer Data will, unless the Buyer agrees otherwise, be based in the UK</li> </ul>
<b>Supplemental requirements in addition to the Call-Off terms:</b>	<p>The Supplier agrees that</p> <p>(a) The definition of “Cloud Content” in the Licence shall be replaced with the following:  “Cloud Content” means any data or other content (including models and related code) that is created or provided by Customer or its Authorised Users, whether directly or indirectly from a third party, for transmission, storage, integration, import, display, distribution or use in or through use of the Cloud Solutions, including any aggregated or transformed versions thereof and any analytical outputs.</p> <p>(b) Notwithstanding anything to the contrary in this Call-Off Contract, clause 18.8 of the Licence applies to Cloud Content and as between the Parties, Buyer retains all rights, title, and interest in and to the Cloud Content. The Supplier agrees to waive or (at Buyer’s option) transfer to Buyer all IPRs in Cloud Content where it vests in Supplier;</p> <p>(c) The provisions of this Call-Off Contract relating to Cloud Content apply to all Cloud Content (as defined above) provided by the Buyer under the Framework call-off contract reference AGEMCSU/TRANS/856 of 12 March 2020.</p> <p>(b) Project Specific IPR does not include any Cloud Content, which shall be dealt with according to this provision and the terms of the Licence;</p> <p>(c) in respect of Buyer Data which is Personal Data that it shall not take or permit Supplier Staff to take any action directed towards the identification of any data subject, the reversal of any pseudonymisation applied to such data, the attribution of personal data to a data subject or the acquisition or processing of any additional information in pursuit of any of those objectives, unless otherwise requested by Buyer as part of Service performance.</p>
<b>Alternative clauses:</b>	None
<b>Buyer specific amendments to/refinements of the Call-Off Contract terms:</b>	<p>The Buyer and the Supplier agree and acknowledge that:</p> <p>(a) Subject to paragraph (b) below, Clause 2 (Grant of Limited Licence) of the Palantir Licence Terms and Conditions (<b>Licence</b>) (as those terms appear in the GCloud Marketplace hosted by CCS) shall apply in full and shall, in the case of any conflict, have precedence over the Framework Agreement and Call-Off Contract. Defined terms in the Licence bear the same meanings where used in this Call-Off</p>



	<p>Contract;</p> <p>(b)</p> <ul style="list-style-type: none"> <li>a. access to the Services other than as set out in Schedule 1 or by any third party is permitted only with the prior written agreement of the Supplier</li> <li>b. The Supplier acknowledges that use of the Services as described in Schedule 1 is use for the Buyer's internal business purposes;</li> <li>c. The Services provide for installation of the Products on Amazon Web Services infrastructure;</li> </ul> <p>(c) Buyer is not permitted to use the Services or any output from them as the basis for any:</p> <ul style="list-style-type: none"> <li>a. decision affecting any particular individual;</li> <li>b. clinical judgment or decision.</li> </ul> <p>(d) The Buyer will comply with applicable Laws in its use of the Services and will not breach any rights of third parties in relation to such use.</p> <p>(e) The Buyer will notify users of the Services of the restrictions on its use set out in these terms.</p> <p>(f) Buyer acknowledges that Supplier is acting as a technology provider and not a clinical decision maker, and Buyer is responsible for making decisions informed by the use of the Products and Services.</p>
<b>Public Services Network (PSN):</b>	Not applicable
<b>Personal Data and Data Subjects:</b>	<p>Confirm whether either Annex 1 or Annex 2 of Schedule 7 is being used:</p> <p>Annex 1</p>

## 1. Formation of contract

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

## 2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the

terms of Framework Agreement number RM1557.11.

(B) The Buyer provided an Order Form for Services to the Supplier.

<b>Signed:</b>	Supplier	Buyer
<b>Name:</b>	[REDACTED]	[REDACTED]
<b>Title:</b>	Authorised Signatory	Chief Financial Officer
<b>Signature:</b>	[REDACTED]	[REDACTED]
<b>Date:</b>	June 11, 2020	11/06/2020

Name [REDACTED]

Title Managing Director

[REDACTED]

Signature [REDACTED]

Date 11/06/2020

## Schedule 1 - Services

The Services to be provided are as set out in the statement of work entered into between the Parties on or around the date this Call-Off Contract and set out in the document below:



PalantirSOWv2.1.doc

x

## STATEMENT OF WORK

Subject to the terms and conditions of G-cloud Call-Off Contract creating this Statement of Work (“**Agreement**”) and for the fees set forth therein, this Statement of Work details the provision of software and services by Palantir for the benefit of the buyer as per the Agreement (“**Customer**”). Unless otherwise specified in this Statement of Work, the capitalized terms used in herein shall have the meaning set forth in the Agreement.

### **1. Provision of Commercial-Off-the-Shelf (COTS) Software**

Palantir Platform – Foundry Cloud Subscription, hosted on Amazon Web Services in the UK region for the term of the Agreement and for the use in relation to the scope described below. The scope of the services below focuses on the configuration of the existing Palantir Foundry COTS software for Customer’s use; no Customer- and project-specific software will be developed under this SOW.

The Customer shall pay for the Infrastructure fee (billed quarterly in arrears).

### **2. Scope of Palantir Services**

In the Phase 1 contract, Palantir stood up a variety of critical services to enable the NHS England and Improvement teams to better understand, prepare and respond to changes in demand for critical resources within the NHS.

This contract will build upon the setup to date within NHS Foundry, so that we do not lose the capability that has been established, but we refine and configure a core set of capabilities within the NHS configured Foundry platform, so that it can be made available and transitioned from development to production as live services. With this in mind, Palantir shall provide the following modules and services during the term of the Agreement, subject to modification by mutual agreement of the Parties in response to evolving Customer priorities and goals. The scope of services will comprise of four key components:

- Provision of Foundry as a NHS data platform – to support data integration, management, analysis, and presentation as a core capability
- Provision of a supply management module for critical items including PPE; Equipment; and ICU Consumables
- An integrated capacity management module to support business planning
- Provision and transition of maintenance of strategic decision makers dashboard

Further details for each service component are provided below:

#### **1. Core Operational Data Integration Platform capability**

Foundry has connected NHS England and Improvement’s data to provide a consistent operating picture - ‘single source of truth’ for the COVID-19 pandemic. A large number of datasets have been integrated into Foundry, including but not limited to:- operational daily situational data and activity data for demand, supply and capacity of critical resources necessary to manage the COVID-19 response.

The integrated data ontology is essential component for providing a consistent data layer from which additional business applications can be developed quickly, thus providing reliable data for consistent operating picture to support decision making. Similarly, integrated modelling that was setup in Phase 1 will form the basis of the modules.

As consistent with the 1<sup>st</sup> phase of work, data within the NHS Data Store and any new data sources as necessary to support the refinement and development of the business applications / modules listed below will be ingested and added to the data ontology for NHS Foundry. Palantir will continue to work with NHS Information Governance leads and the defined Front Door process in performing a low-friction analysis of the proportionality and purpose for the use of the data.

All access to data will be under strict technical controls and limit the use of data within NHS Foundry exclusively for NHSE/I approved purposes and by NHSE/I approved personnel.

Palantir will continue to ensure the maintenance of the Data Ontology, processing and integration along with the security architecture, working closely with the NHSE/I data services team to support knowledge transfer.

## **2. Supply Management**

This module will build on the data ontology, workflow and functionality that was developed for managing the supply and demand of critical resources including PPE, ventilation and oxygen equipment and ICU consumables. The scope of service will be to refine the configuration the module to support end-to-end management of these critical resources, so that they enable collaboration between federated teams working across the supply chain using Foundry to provide a clear operating picture of supply and demand. The module will include provision of management information and workflow functionality between national, regional, and local organisations and or systems to enable business users to track stock, support allocation, mutual aid.

*Key user groups:*

- Trust procurement cells
- Regional leads
- Supply chain leads

## **3. Business Planning**

This module will build on the data ontology, user interface and integrated modelling functionality that was setup in Phase 1 to support integrated demand and supply modelling to support planning. The scope of service will be to refine, further integrate and improve the configuration of this module to support collaborative business planning between National, Regional, and local systems (STP). The functionality will include workflow and user interfaces and functionality to collect and support integration of local system and or trust data for planning purposes.

The module will enable:

- National teams to set and share common planning assumptions and scenarios within the application
- Regional and local system users to adjust set parameters within the module, and submit, and export model outputs for specific local scenarios
- Integration of local trust level data to provide inputs to the core planning scenarios
- Ability to create national, regional and system level plans through aggregation of modelling outputs and or local data to support analysis and pinpoint variation and outliers to central planning model outputs and assumptions.
- Iterative planning cycles between national, regional and local systems using common operating picture of the changes and final agreed position, to enable tracking against the plan.
- Use of the existing functionality to export outputs for users to use modelling outputs for local analysis and onward sharing with partner organisations

The functionality listed above is not meant to be exhaustive and will be finalised with business users as quick iterative configuration sprints with business users as part of configuration of the integrated business modelling module.

*Key user groups:*

- Integrated Planning Tool users: STP level users completing Phase 3 plans (and Regional users where appropriate)
- Ongoing Monitoring Tool: National, Regional and STP level users

#### **4. Provision of the Strategic Dashboard**

The Strategic Decision Makers Dashboard has provided a unifying product for executives across the health and care system. The scope of service for this product will be complete the development activity necessary to provide specific views of data in accordance to the agreed access rules, and to continue provision of automated feeds from Foundry to provide the daily updates to the Civil Contingencies Secretariat for integration into their local dashboard. The scope of service will be for Palantir to provide training to, and work with, NHSEI team to transition the maintenance of the dashboard.

*Key user groups:* Dashboard will be used by:

- NHS E/I executives
- For consumption of the Civil Contingencies Secretariat division of the Cabinet Office
- Key Regional and Trust level decision makers expressly authorised to access the Dashboard by NHS E/I executives

### **3. Core service requirements across all NHS Foundry components above**

As part of the scope of services for Foundry, Palantir will also provide:

- Most effective data engineering and configuration of Foundry to enable successful implementation of the services and modules set out above
- Provision of product documentation, coding and other necessary platform-based self-serve training for NHSEI staff to fully operate Foundry
- Provision of relevant training materials and library of documentation for general user education, troubleshooting and best practice guidance for development
- L2-3 Issue resolution for Foundry support questions for up to 1500 users and if necessary, handoff support to the L1 support provider
- All service modules will be delivered in collaboration with the business owners for each module and the Senior Responsible Officer for Foundry.

### **4. Customer Dependencies**

Customer shall provide necessary and reasonable assistance to Palantir for the provision of Palantir services. Palantir's provision of the services set forth above and compliance with requirements herein, including its ability to timely meet any timelines or milestones or timely provide any agreed upon software capabilities, training, or support, are contingent upon Customer's timely and full provision of the following ("**Customer Dependencies**"):

- *Data Access*
- Timely access to or provisioning of relevant data
- Timely access to or provisioning of necessary network components for the purposes of data ingestion and integration
- Timely information governance approvals required for the use of relevant data
- Making sure that the provision and use of data complies with the applicable law and policies and, if needed, anonymising/pseudonymising personal data (if any)
- *User and SME Access*
- Timely provision of technical personnel for data integration, pipeline and ontology maintenance and data analytics

- Timely access to Customer test users and subject matter experts for implementation and configuration support
- Timely assistance from Customer's technical experts, data owners to ensure proper operation of the Cloud Solution with Customer data and technology systems and infrastructure
- Provision of L1 response and triage service for Issues support
- Provision of technical personnel that can delivering training

Palantir shall communicate deficiencies in necessary Customer Dependencies in a timely manner so that Customer can find and assign appropriate resources and resolve blocking problems.

#### **5. Project Management/Governance**

The programme will be accountable to the National CFO for NHS England and Improvement. The Senior Responsible Officer for this programme will be the NHS England and Improvement Director of Data & Analytics. The programme governance structure will be explained at the start of the programme and will include representatives of both Customer and Palantir to provide advice on technical feasibility.

## 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:

- Palantir Foundry: <https://www.digitalmarketplace.service.gov.uk/g-cloud/services/501000199851013>
- Item 31 PILOT / TRIAL with scope based on your requirements set out in Schedule 1 and subject to nominal fee of GBP 250,000 per month plus VAT for the licence. Labour is being provided on a pro-bono basis, so SFIA rate card rates shall not apply.
- Infrastructure fees charged quarterly (if any)



## 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.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

### 2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
  - 4.1 (Warranties and representations)
  - 4.2 to 4.7 (Liability)
  - 4.11 to 4.12 (IR35)
  - 5.4 to 5.5 (Force majeure)
  - 5.8 (Continuing rights)
  - 5.9 to 5.11 (Change of control)
  - 5.12 (Fraud)
  - 5.13 (Notice of fraud)
  - 7.1 to 7.2 (Transparency)
  - 8.3 (Order of precedence)
  - 8.4 (Relationship)
  - 8.7 to 8.9 (Entire agreement)
  - 8.10 (Law and jurisdiction)
  - 8.11 to 8.12 (Legislative change)
  - 8.13 to 8.17 (Bribery and corruption)
  - 8.18 to 8.27 (Freedom of Information Act)
  - 8.28 to 8.29 (Promoting tax compliance)
  - 8.30 to 8.31 (Official Secrets Act)
  - 8.32 to 8.35 (Transfer and subcontracting)
  - 8.38 to 8.41 (Complaints handling and resolution)
  - 8.42 to 8.48 (Conflicts of interest and ethical walls)
  - 8.49 to 8.51 (Publicity and branding)
  - 8.52 to 8.54 (Equality and diversity)
  - 8.57 to 8.58 (data protection)

- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

3.1 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.

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

3.3 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**

3.4 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.

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

### **4. Supplier staff**

4.1 The Supplier Staff must:

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

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

## **5. Due diligence**

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

## **6. Business continuity and disaster recovery**

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

## 7. Payment, VAT and Call-Off Contract charges

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

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

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

## 9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

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

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

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

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

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

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

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

## **10. Confidentiality**

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

## **11. Intellectual Property Rights**

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
- rights granted to the Buyer under this Call-Off Contract
  - Supplier's performance of the Services
  - use by the Buyer of the Services
- 11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

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

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

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

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

## 12. Protection of information

12.1 The Supplier must:

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

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

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

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

## 13. Buyer data

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

- 13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
- 13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.
- 13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
  - the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
  - guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
  - the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/collection/risk-management-collection>
  - government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
  - the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
- 13.6 The Buyer will specify any security requirements for this project in the Order Form.
- 13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.



- 13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer Data.

## **14. Standards and quality**

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

## **15. Open source**

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

## **16. Security**

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

- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
  - Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

## 17. Guarantee

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

## 18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

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

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

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

## **19. Consequences of suspension, ending and expiry**

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

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

- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- any rights, remedies or obligations accrued before its Ending or expiration
  - the right of either Party to recover any amount outstanding at the time of Ending or expiry
  - the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data); 19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
  - any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires
- 19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:
- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
  - return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
  - stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
  - destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
  - work with the Buyer on any ongoing work
  - return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
- 19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
- 19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

## 20. Notices

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

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

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

## 21. Exit plan

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

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls

process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

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

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

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

## **22. Handover to replacement supplier**

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

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- other information reasonably requested by the Buyer

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

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

## **23. Force majeure**

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

## **24. Liability**

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

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

## **25. Premises**

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

## **26. Equipment**

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

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

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

## **28. Environmental requirements**

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



## 29. The Employment Regulations (TUPE)

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

representatives.

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

## **30. Additional G-Cloud services**

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

## **31. Collaboration**

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

## **32. Variation process**

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

Variation.

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

### **33. Data Protection Legislation (GDPR)**

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

**Schedules 3 – 5**

**NOT USED**

## Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
<b>Audit</b>	An audit carried out under the incorporated Framework clauses specified by the Buyer in the Order (if any).
<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes</li> <li>created by the Party independently of this Call-Off Contract, or</li> </ul> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.
<b>Buyer Software</b>	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
<b>Call-Off Contract</b>	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
<b>Commercially Sensitive Information</b>	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
<b>Confidential Information</b>	<p>Data, personal data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> <li>information about business, affairs, developments, trade secrets,</li> </ul>

	<p>know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above</p> <ul style="list-style-type: none"> <li>other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
<b>Controller</b>	Takes the meaning given in the GDPR.
<b>Crown</b>	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
<b>Data Loss Event</b>	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
<b>Data Protection Impact Assessment</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
<b>Data Protection Legislation (DPL)</b>	<p>Data Protection Legislation means:</p> <ul style="list-style-type: none"> <li>i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time</li> <li>ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy;</li> <li>iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .</li> </ul>
<b>Data Subject</b>	Takes the meaning given in the GDPR
<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract</li> </ul> <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
<b>Deliverable(s)</b>	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
<b>Digital Marketplace</b>	The government marketplace where Services are available for Buyers to buy. ( <a href="https://www.digitalmarketplace.service.gov.uk/">https://www.digitalmarketplace.service.gov.uk/</a> )
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant

	Government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: <a href="http://tools.hmrc.gov.uk/esi">http://tools.hmrc.gov.uk/esi</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.
<b>Force Majeure</b>	<p>A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure</li> <li>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>• any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</li> </ul>
<b>Former Supplier</b>	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).
<b>Framework Agreement</b>	The clauses of framework agreement RM1557.11 together with the Framework Schedules.
<b>Fraud</b>	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.
<b>Freedom of Information Act or FoIA</b>	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.
<b>G-Cloud Services</b>	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.

<b>GDPR</b>	The General Data Protection Regulation (Regulation (EU) 2016/679).
<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
<b>Government Procurement Card</b>	The Government's preferred method of purchasing and payment for low value goods or services <a href="https://www.gov.uk/government/publications/government-procurement-card--2">https://www.gov.uk/government/publications/government-procurement-card--2</a> .
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
<b>Implementation Plan</b>	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
<b>Indicative Test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information Security Management System</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
<b>Insolvency Event</b>	Can be: <ul style="list-style-type: none"> <li>● a voluntary arrangement</li> <li>● a winding-up petition</li> <li>● the appointment of a receiver or administrator</li> <li>● an unresolved statutory demand</li> <li>● a Schedule A1 moratorium.</li> </ul>
<b>Intellectual Property Rights or IPR</b>	Intellectual Property Rights are: <ul style="list-style-type: none"> <li>● 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</li> <li>● 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</li> <li>● all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>
<b>Intermediary</b>	For the purposes of the IR35 rules an intermediary can be: <ul style="list-style-type: none"> <li>● the supplier's own limited company</li> <li>● a service or a personal service company</li> <li>● a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
<b>IPR Claim</b>	As set out in clause 11.5.



<b>IR35</b>	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
<b>IR35 Assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
<b>Law</b>	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
<b>LED</b>	Law Enforcement Directive (EU) 2016/680.
<b>Loss</b>	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 ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement section 6 (What you report to CCS).
<b>Material Breach</b>	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
<b>New Fair Deal</b>	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
<b>Order</b>	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an Order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.

<b>Personal Data</b>	Takes the meaning given in the GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the GDPR.
<b>Processing</b>	Takes the meaning given in the GDPR.
<b>Processor</b>	Takes the meaning given in the GDPR.
<b>Prohibited Act</b>	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
<b>Project Specific IPRs</b>	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory Body or Bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant Person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the Employment Regulations applies.
<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
<b>Replacement Supplier</b>	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
<b>Security Management Plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Service Data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.

<b>Service Definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
<b>Service Description</b>	The description of the Supplier service offering as published on the Digital Marketplace.
<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
<b>Spend Controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start Date</b>	The start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
<b>Subcontractor</b>	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
<b>Supplier Staff</b>	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
<b>Supplier Terms</b>	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.
<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).
<b>Working Days</b>	Any day other than a Saturday, Sunday or public holiday in England and Wales.
<b>Year</b>	A contract year.

## Schedule 7 - GDPR Information

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

### Annex 1 - Processing Personal Data

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

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

Description	Details
Identity of Controller for each Category of Personal Data	<p><b>The Buyer is Controller and the Supplier is Processor</b></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 Personal Data provided by the Buyer (or at the direction of the Buyer) for the purposes of the delivery by the Supplier of the Services, as set out in the Statement of Work ("SOW"):</p> <p>Nature and purpose of Processing</p> <p>Data Processed in accordance with the Agreement may be subject to the following Processing activities:</p> <ul style="list-style-type: none"> <li>• performance by Palantir of activities necessary to provide products or services or otherwise perform its obligations under the Agreement;</li> <li>• disclosures in accordance with the Agreement, or as compelled by law.</li> </ul>
Duration of the Processing	<p><i>The Term of the Agreement (as set out in the Call-Off Order Form for this Agreement) plus the period from the expiry of the Term until the return or deletion of all Customer Personal Data by the Supplier in accordance with the Agreement and applicable law.</i></p>

<p>Nature and purposes of the Processing</p>	<p><i>Data Processed in accordance with the Agreement may be subject to the following Processing activities:</i></p> <ul style="list-style-type: none"> <li>• <i>performance by the Supplier of activities necessary to provide products or services or otherwise perform its obligations under the Agreement;</i></li> <li>• <i>disclosures in accordance with the Agreement, or as compelled by law</i></li> </ul> <p><i>The specific purposes for the processing are described below</i></p> <p><i>The aim of the project is to create a data store which will be used to:</i></p> <ol style="list-style-type: none"> <li>1. <i>Track and predict the spread of COVID-19;</i></li> <li>2. <i>Model interventions including guidance for public &amp; patients;</i></li> <li>3. <i>Optimise health &amp; community resources.</i></li> </ol> <p><i>Processing many &amp; varied data sources is critical for achieving these aims.</i></p> <p><i>The processing will primarily focus on data triangulation to support tracking, surveillance and reporting for Covid-19.</i></p> <p><i>As Covid-19 is now a pandemic and to ensure that we are taking a data led approach, there are key questions which will need to be answered:</i></p> <ol style="list-style-type: none"> <li>1. <i>How do we track the spread of COVID 19 and the impact of it?</i></li> <li>2. <i>How do we predict the spread of COVID 19 and the impact of it?</i></li> <li>3. <i>How do we understand the impact of interventions?</i></li> <li>4. <i>How do we optimise the use of resources across the Healthcare System?</i></li> <li>5. <i>How do we equip the public with the resources and tools they need, to help themselves?;</i>The above are the primary purposes for which the data will need to be processed.</li> </ol>
<p>Type of Personal Data</p>	<p><i>In order to provide the Services or otherwise perform its obligations under the Agreement, the Supplier will process the Personal Data provided or made available to the Supplier in relation to the Agreement.</i></p> <p><i>The Supplier is granted access to Personal Data only after an aggregation and de-identification process meeting NHS standards, and is under a contractual restriction precluding identification of data subjects.</i></p>

<p>Categories of Data Subject</p>	<p><i>Data Subjects include the individuals about whom data is provided to the Supplier via the Services or otherwise by (or at the direction of) the Buyer or Buyer's users who are authorised to use the Services. These may include, but are not limited to, the following: (i) Employees, contractors, or agents of the Buyer (who are natural persons); (ii) the Buyer's users authorized to use the Service; (iii) the Buyer's clients, customers, or other users of the Buyer's products or services; and/or (iv) Third parties with which the Buyer conducts business and in each case, they include former, present, and/or prospective individuals in these categories.</i></p> <p><i>Members of the public</i></p> <p><i>Patients</i></p>
<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p><i>Notwithstanding anything else in the Framework Agreement and / or the Call-off Contract, The Parties agree that the terms of the Supplier's terms "STANDARD EU CONTRACTUAL CLAUSES (PROCESSORS)" below shall apply to this Agreement.</i></p>

## STANDARD EU CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

NHS England acting through NHS Arden & GEM CSU (a business unit of National Health Service Commissioning Board of Skipton House, 80 London Road, London, SE1 6LH), referred to as the “Buyer” in the Agreement, on behalf of itself and other entities it may receive data from or provide access to Palantir’s software and services to.

(each a “**data exporter**”)

And

Name of the data importing organisation:

Palantir Technologies Inc., on behalf of itself and as an agent for and on behalf of all legal entities it directly or indirectly controls located outside of the European Economic Area, and which are from time to time serve as data processors in respect of the personal data processed by or on behalf of the data importer.

Address: 100 Hamilton Ave., Suite 300, Palo Alto, CA 94301

(the “**data importer**”)

each a “**party**”; together the “**parties**”,

HAVE AGREED on the following Contractual Clauses (the “**Clauses**”) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

### Clause 1

#### **Definitions**

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system

ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## *Clause 2*

### ***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## *Clause 3*

### ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.



## Clause 4

### ***Obligations of the data exporter***

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

## Clause 5

### ***Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## *Clause 6*

### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data

exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

#### *Clause 7*

##### ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### *Clause 8*

##### ***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

#### *Clause 9*

##### ***Governing Law***

The Clauses shall be governed by the law of the Member State in which the relevant data exporter is

established.

## *Clause 10*

### ***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

## *Clause 11*

### ***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the relevant data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the relevant data exporter's data protection supervisory authority.

## *Clause 12*

### ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of a data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

## **APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES [CONFIDENTIAL]**

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

### **Data exporter**

The data exporter is, a public body that is identified in the Agreement.

### **Data importer**

The data importer is a software company (including, where applicable, its subsidiaries and affiliates) which may from time to time process personal data upon the instruction of the data exporter in accordance with the terms of these Clauses and the G-Cloud Framework Agreement and Call-Off Contract entered into by (1) Palantir Technologies UK Limited and (2) the Department of Health and Social Care (the "Agreement").

### **Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

The data subjects are users of software and services.

### **Categories of data**

The personal data transferred concern the following categories of data (please specify):

- The data to be processed may include, but is not limited to:
  - Email, login and usage information required for the provision of software and services.

### **Special categories of data (if appropriate)**

- The personal data transferred concern the following special categories of data (please specify):
  - The data importer does not access sensitive personal data in the ordinary performance of the services. Notwithstanding the foregoing, the data importer may access sensitive personal data only where such access is lawful and critical in the provision of the services.

### **Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

Data analytics, problem solving and data hosting and maintenance services, as defined and pursuant to the Agreement and these Clauses .

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES [CONFIDENTIAL]**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The data importer will maintain appropriate administrative, physical, technical, and organizational measures against unauthorised or unlawful processing of, accidental loss, destruction or damage to, and for protection of the security, confidentiality, and integrity of personal data, including any requirements relating to such measures set out in the Agreement between the parties.

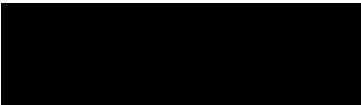
**DATA EXPORTER**

**DATA IMPORTER**

Name:

Name:  .....

Authorised Signature:

Authorised Signature 

## Annex 2 – NOT USED