Crown Commercial Service

G-Cloud 12 Call-Off Contract

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

Part A - Order Form

Digital Marketplace service ID number:	309622252630434
Call-Off Contract reference:	
Call-Off Contract title:	Diligent Board Portal
Call-Off Contract description:	Licence to board meeting management software
Start date:	23rd January 2022
Expiry date:	22nd January 2023
Call-Off Contract value:	£[redacted] per year
Charging method:	Annual Invoice
Purchase order number:	

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

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

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

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

From: the Buyer	Competition and Markets Authority The Cabot, 25 Cabot Square, London, E14 4QZ [redacted]
To: the Supplier	Diligent Boardbooks Limited 0207 605 7438 1 Strand Trafalgar Square, London WC2N 5HR Company number: 06029195
Together: the 'Parties'	

Principle contact details

For the Buyer:	Name: [redacted] Email: [redacted] Phone Number: [redacted]

For the Supplier:	Title: [redacted] Name: [redacted] Email: [redacted] Phone: [redacted]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on the start date set forth above and is valid for 24 months.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for disputed sums or at least 30 days from the date of written notice for Ending without cause. In the event of any Ending without cause, the Ending shall take effect no sooner than the anniversary of the start date, it being understood that all fees paid or payable are non-refundable and due in full except where the Call-Off Contract is terminated for cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for three period(s) of 12 months each, by giving the Supplier 30 days written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud Lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud software
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: [redacted]
Additional services:	Training for all users to be provided.
Location:	The Services will be delivered to locations throughout the United Kingdom via users' devices.
Quality standards:	Not used.
Technical standards:	The technical standards required for this Call-Off Contract are: [redacted]
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as follows: **DILIGENT BOARDS** **SERVICE LEVEL COMMITMENT**

- The following describes the minimum standards for availability of the Diligent Service.

System Availability

The Diligent Service will be available at least 99.5% of the time in any calendar month. Availability is determined by dividing the duration of "Service-Affecting Outages" by the total number of minutes in a calendar month and subtracting the resulting decimal number from 1.000. A Service-Affecting Outage shall be deemed to have occurred when the Diligent Boards Site is not available to Client except that outage time resulting from any of the following causes shall not be considered when determining the percentage of Availability:

1. Outages caused by failure in Client's operating environment (including Client's connectivity to the Diligent Service);

2. Outages for scheduled maintenance provided that such maintenance is scheduled during the hours of 10PM Friday – 5AM Saturday CET. Diligent Service maintenance is ordinarily carried out so that it will not interfere with the availability of the Diligent Service. Diligent may revise the times at which scheduled maintenance may be performed by providing Client with at least thirty (30) days prior written notice of such revision.

3. Outages for emergency maintenance that Diligent determines is reasonably necessary;

4. Outages that occur as a result of a Force Majeure Event; and

5. Outages during a transition to the disaster recovery site following a disaster.

System Availability Credits

If the system level availability is between:

(a) Ninety-nine and forty-nine hundredths percent (99.49%) to ninety-five percent (95%) in any given calendar month, Client shall receive a credit equal to ten percent (10%) of that month's Subscription Fees, being 1/12 of the annual Subscription Fee;

(b) Ninety-four and nine tenths percent (94.9%) and below in any given calendar month, Client shall receive a credit equal to twenty-five percent (25%) of that month's Subscription Fees, being 1/12 of the annual Subscription Fee.

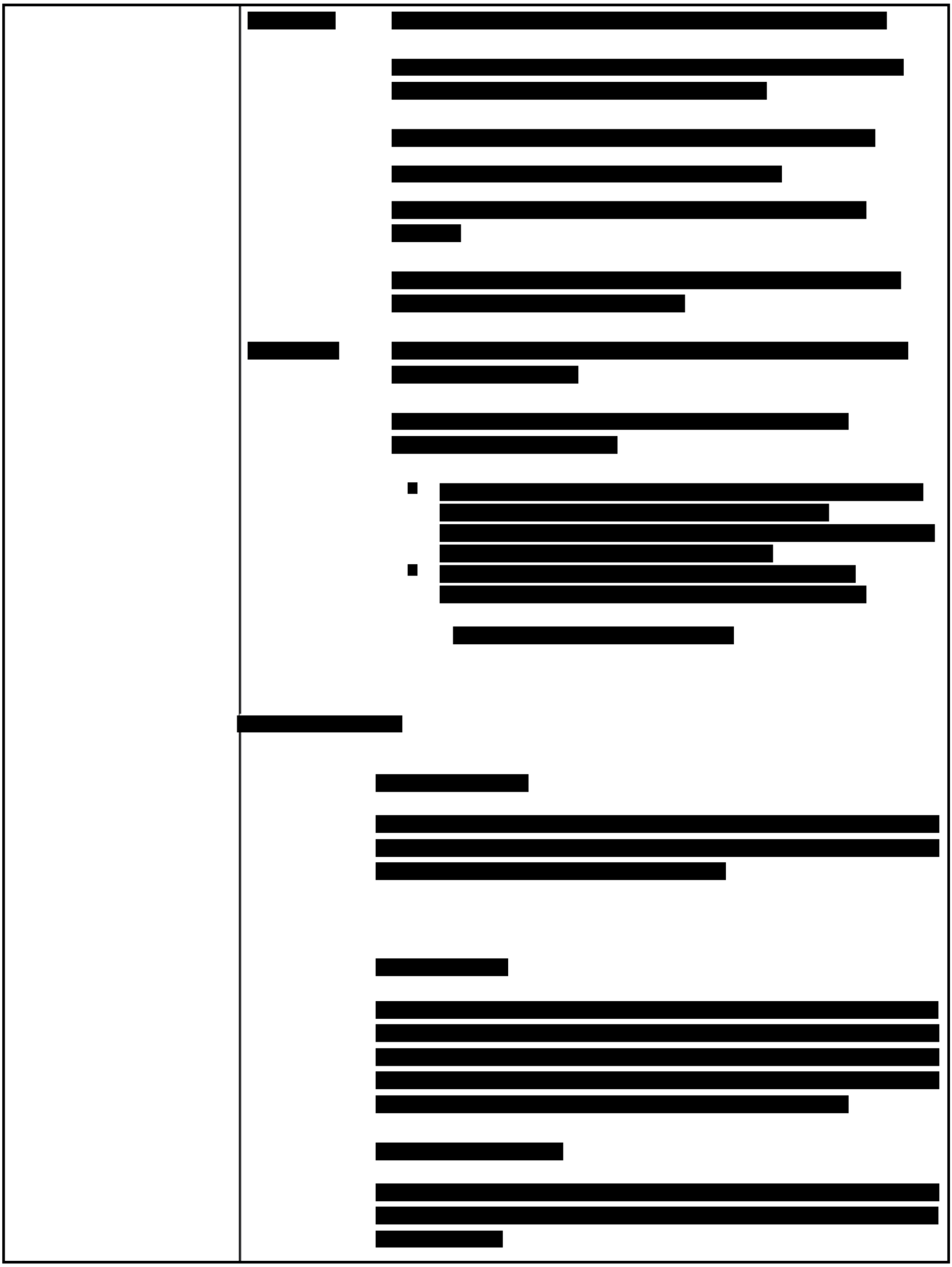
If Diligent fails to reach the 99.5% level in three of any twelve consecutive calendar months Client shall have the option to terminate this Agreement per the terms and conditions governing this Agreement.

If a Service-Affecting Outage occurs, Diligent will promptly respond upon receipt of notice from the Client. Diligent will attempt to achieve resolution of the Service-Affecting Outage as soon as possible but in no event longer than eight (8) hours from receipt of notice. The foregoing notwithstanding, in the event a software fix is required, this could take up to forty-eight (48) hours to implement, but this would be a rare occurrence. In such event, a work-around will be implemented, pending the software fix.

[redacted]

	[redacted]
Onboarding:	The onboarding plan for this Call-Off Contract is as follows: **IMPLEMENTATION PLAN** **Online Access** The proposed implementation schedule below is a sample for planning purposes, and will be further detailed and tailored to Client's unique requirements as Diligent gains a better understanding of Client's requirements. Implementation and training can begin within one week of Diligent's receipt of User surveys. The implementation process begins with a kick-off meeting at which the Client's team agrees on dates, timelines, and contact persons. Diligent recommends that administrative training be divided into two or three one-hour sessions, over a period of 2 -3 weeks. This ensures that Users have plenty of opportunity to learn at their own pace. [redacted]

[redacted]



	[redacted]
Offboarding:	Offboarding shall occur as follows: After termination of this Agreement, Diligent will notify Client of the deletion date for Client Data on Diligent production systems. Within sixty (60) days of such deletion date, any backups of Client Data shall be deleted. During the Term, Client will be able to download a copy of Client Data in PDF format.
Collaboration agreement:	Not used.
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed 125% of the total fees paid or payable to the Supplier during the Call-Off Contract Term. The annual total liability for Buyer Data defaults will not exceed the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.
Insurance:	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. Upon request, Supplier shall provide copies of invoices, contract documentation and other relevant documentation to support fees charged under this Agreement. **Costs of conducting audits or inspections** 7.13 Each Party is responsible for covering all their own other costs incurred from their compliance with these audit obligations.

Buyer's responsibilities:	The Buyer is responsible for ensuring staff are available for training sessions and provision of a room for training, unless training takes place by WebEx.
Buyer's equipment:	The Buyer's equipment to be used with this Call-Off Contract includes computers, laptops and tablet devices for all users. For the avoidance of doubt, the Buyer shall provide all Hardware needed for Buyer's users to make use of the Diligent Boards service. Reason: hardware required for use of service.

Supplier's information

Subcontractors or partners:	The following is a list of the Supplier's Subcontractors or Partners. Not applicable.

Call-Off Contract charges and payment

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

Payment method:	The payment method for this Call-Off Contract is by BACS.
Payment profile:	The payment profile for this Call-Off Contract is annually in advance.
Invoice details:	The Supplier will issue electronic invoices in annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent preferably by email to: [redacted] or by post to: Competition and Markets Authority, The Cabot, 25 Cabot Square, London
Invoice information required – for example purchase order, project reference:	All invoices must include a valid purchase order number, provided that such purchase order number must be provided to the Supplier in advance of when invoices are to be issued. The invoice for the first year of the Call-Off Contract is typically sent on or around date of last signature. Additional years are typically sent thirty (30) days prior to each anniversary of the start date.
Invoice frequency:	Invoice will be sent to the Buyer annually.
Call-Off Contract value:	The total value of this Call-Off Contract is [redacted] per year
Call-Off Contract charges:	The breakdown of the Charges is PRICING AND FEES

Configuration of Sites, Committees, and Users as of the Effective Date			
Accessing Entities and Individuals	Qty	Price Each	Total
• [redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the implementation plan, exit and offboarding plans and milestones outlined above, subject at all times to the Buyer providing reasonable support to enable Supplier to meet such obligations and execution of this Call-Off Contract.
Guarantee:	Not used.
Warranties, representations:	Not used.
Supplemental requirements in addition to the Call-Off terms:	Not used.
Alternative clauses:	Not used.
Buyer specific amendments	Not used.

[redacted]

to/refinements of the Call-Off Contract terms:	
Public Services Network (PSN):	Not used.
Personal Data and Data Subjects	Schedule 7 will be used.

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 RM1557.12.

(B) The Buyer provided an Order Form for Services to the Supplier as set out in Part A.

Signed:	Supplier	Buyer
Name:	[redacted]	[redacted]
Title:	[redacted]	[redacted]
Signature:	[redacted]	[redacted]
Date:	February 14, 2022 | 8:14 AM EST	11th February 2022

Schedule 1 - Services

Overview

The Diligent Service known as Diligent Boards provides an internet-based portal that enables Client to manage its board and other materials through a site dedicated to Client Data (Client's "**Diligent Boards Site**"). Client's Diligent Boards Site is a secured location in the Diligent Service which is designed to be accessed only by authorized Users with a unique User ID and password. The Client's administrative staff prepares the board materials, which are then uploaded through the Diligent OneClick application. Those materials are then converted by the Diligent Service so that they can be accessed

and viewed by Users electronically, in a format that can be accessed through the Client Software or a standard web browser. Available access rights are set forth in Sections 1, 2 and 3 below, and the Order reflects Client's chosen access rights. For clarity, Content Services are separate from Diligent Boards and are not within scope of this Exhibit.

1. Assigned Groups

Site: A Diligent Boards Site for a number of Users of the Diligent Service with access to a set of uploaded materials.
Committee: A meeting group within the Site that permits more limited access to certain materials for a particular group of Users.

2. User Types

Users (Board Members/Executives): Users with the ability to view the Client's documents using a supported web browser or Client Software.
Administrators: Users with the ability to upload, collate, print, view, approve and publish Client's Board and Committee documents.

3. Additional Capabilities

D&O Questionnaires Module: This module provides seamless questionnaire integration.
Messenger: This module adds messaging functionality for Users through the Diligent Messenger Client Software.
Evaluations Questionnaires Module: This module provides survey capability for the purpose of board evaluations, and automated reporting and analysis of the data gathered from the surveys.
Minutes Module: This module enables Client to enhance minute taking with a tool that is integrated with Diligent Boards and enables Client to take minutes and assign action items.
Diligent Nominations: This Content Service is separate from but supplements the Diligent Boards service offering by providing proprietary governance analytics and information about companies and individuals.

For the avoidance of doubt, only those access rights listed in the Order are included in the pricing selected under this Agreement. For the avoidance of doubt, future additional access rights offering new functionality may be made available at additional cost. A Diligent representative can provide pricing for access rights not listed in the Order.

4. Access for Administrators

The Diligent Service allows all designated Administrators, i.e., the company secretary and administrative personnel, to upload, collate, print, view, approve and publish the Client's board and committee documents.

Configuration of this feature includes:

- Set-up and customization of the Client's Diligent Boards Site for use by Administrators, including:
  - Project planning meeting, including review of current work flow and identification of key milestones, leading to development of an implementation plan that fits Client's needs and priorities

- Collection of User survey information, mapping board and committee membership

- Creation of a dedicated Diligent Boards Site

- Creation and configuration of User accounts
- Configuration of password policy and security configuration

- Installation of Diligent OneClick
- Configuration and installation of off-line features on the Administrator's laptop computer

5. Online and Offline Access for Users

While online, Users can view the Client's documents using a supported web browser or the Client Software. Each User can access the Diligent Boards Site with a User ID through the Client Software and supported web browsers.

Offline functionality allows Users to download materials from the Client's Diligent Boards Site via the internet and view them using the Client Software when the internet is not accessible. Configuration of this feature includes the capability to securely download and store an encrypted version of Client's materials to a designated laptop or supported mobile device and view materials when not connected to the internet.

6. Implementation Process

After execution of this Agreement, Diligent will assign an account management team to work with and train Client's Users in accessing and using the Diligent Service. The goal is to work directly with Client to streamline the process of preparing, approving and delivering board materials to deliver a system that the Users (regardless of their technological expertise) will quickly, easily and enthusiastically embrace and use. A sample implementation plan is included at the end of this Exhibit.

Diligent's one-on-one approach to the implementation process for the Diligent Service includes:

- Review of the present board preparation, workflow, and approval processes
- A technical profile of each User
- Recommended implementation strategy for Users based on their individual level of technological expertise and Client's objectives
- Ongoing general consulting regarding board material preparation and distribution

7. Training and Support

Diligent training for Users includes:

- Separate training session(s) for the Administrators. Training includes instruction on log-in procedures, password usage, creating and building a Diligent Service file/database, editing and making changes, and uploading/converting files into the Diligent Service format for easy viewing by Users
- A separate training session for Users who wish to become familiar with the Diligent Service technology prior to the first board meeting

- One-on-one web training sessions with Users
- Ongoing training, including training for new Users, on-site or via web-conferencing, on an as-needed basis
- User guides for quick, easy reference.

Diligent's "Concierge" level of support reflects its understanding of the importance of being available 24/7/365 to assist every User and provide them with the comfort of knowing that Diligent is listening and responding to their needs, concerns and requirements.

- All Users have 24/7/365 personal assistance, via a toll-free number, to receive any help they need as well as answers to any Diligent application-related questions, at no additional cost.
- Remote diagnostics and troubleshooting (including network and firewall issues) is provided for each User anywhere, anytime, as needed, at no additional cost.

8. Updates

Updates to the Diligent Service and Client Software are included **at no additional cost**.

9. Failover / Backup

The Diligent Service includes a fault tolerant system configuration that is included **at no additional cost**. Client Data will reside on the Client's Diligent Boards Site in a primary data center, which is replicated to a secondary data center every four hours. Each data center is capable of delivering the Diligent Service. Additionally, each data center is built with hardware and network redundancy to offer continuous delivery of the Diligent Service. System availability is continuously monitored and failover is initiated if a primary data center becomes unavailable.

10. Security

Diligent uses encryption algorithms, consistent with generally-accepted standards and practices adopted and implemented by software-as-a-service ("SAAS") providers, designed to limit unauthorized access to Client Data. Each User will have a unique User ID and password which will be required for the User to access Client's Diligent Boards Site. Diligent enforces password strength requirements, including frequency of password changes, according to Client's request.

Diligent uses a layered approach to security architecture, making use of firewalls, intrusion prevention systems, reverse web proxies, and segregation of specific application functions to provide security and integrity of the overall environment.

Upon request, more detailed information on Diligent's extensive security measures and protocols can be provided. Technical questions may be addressed to the appropriate salesperson or account management teams, who will engage the appropriate persons from Diligent's network, security and operational departments.

Clients may also elect to turn on two factor capability/device authorization for Users. These features offer enhanced security for Users accessing the Diligent Service by requiring additional verification of a User's identity (beyond User ID and password). This can be by means of a separate two factor token or via the User's device itself. For the avoidance of doubt, two factor tokens are available solely for the PC for an additional fee, while Device Authorization, offering authentication for the iPad and other supported devices, is available at no additional cost.

11. Client Requirements

In order to use the Diligent Service, Client and Users must satisfy Diligent's minimum technology requirements, which, as of the Effective Date, are available at www.diligent.com/tech-specs. The URL where such requirements are stored may change, but a current version of Diligent's minimum technology requirements is available from Diligent at any point upon request. All subscription costs for wireless and WiFi services must be covered by the Client / User.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			[redacted]
ONE-TIME INSTALLATION FEE (set-up, installation and training for above configuration)			**£0.00**

[redacted]

[redacted]			
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

Part B - Terms and conditions

1. Call-Off Contract start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)

[redacted]

- 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)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

5. Due diligence

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier

must notify the Buyer within 10 Working days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

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

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

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

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

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Act (DPA) or under incorporated Framework Agreement clauses 8.83 to 8.91. 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 Accreditation of Information Systems 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/guidance/risk-management-collection
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

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

13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer

immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use 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 the notice to the Supplier specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

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

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

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

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

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

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

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

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

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

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

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

22. Handover to replacement supplier

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

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

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

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for

replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

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

23.1 than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

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

25. Premises

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

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

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

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

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

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer’s request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- the activities they perform
- age
- start date

- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

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

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date in the form set out in Schedule 3.

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 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional processing if permitted by Law).

33.2 The Supplier will provide all reasonable assistance to the Buyer to prepare any Data Protection Impact Assessment before commencing any processing (including provision of detailed information and assessments in relation to processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.

33.3 The Supplier must have in place Protective Measures, which have been reviewed and approved by the Buyer as appropriate, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Personnel only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier Personnel with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier's obligations under this Clause;

ii) are subject to appropriate confidentiality undertakings with the Supplier or relevant Subprocessor

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

33.5 The Supplier will not transfer Personal Data outside of the European Economic Area unless the prior written consent of the Buyer has been obtained and

i) the Buyer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Buyer;

ii) the Data Subject has enforceable rights and effective legal remedies;

iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Buyer in meeting its obligations); and

iv) the Supplier complies with any reasonable instructions notified to it in advance by the Buyer with respect to the processing of the Personal Data.

33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

33.7 The Supplier will notify the Buyer immediately if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation in accordance with any timescales reasonably required by the Buyer.

33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

i) the Buyer determines that the processing is not occasional;

ii) the Buyer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

iii) the Buyer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

i. 33.9 Before allowing any Subprocessor to process any Personal Data related to this Call-Off Contract, the Supplier must obtain the prior written consent of the Buyer, and shall remain fully liable for the acts and omissions of any Subprocessor.

33.10 The Buyer may amend this Call-Off Contract on not less than 30 Working Days' notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 3 - Collaboration agreement - Not used

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 4 - Alternative clauses – Not used

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 5 – Guarantee – Not used

The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.

Collaboration Agreement	An agreement between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the Data Protection Legislation.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach.
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
Data Protection Legislation	Data Protection Legislation means: i) all applicable Law about the processing of personal data and privacy; and ii) ii) The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive)

	Regulations 2003 including if applicable legally binding guidance and codes of practice issued by the Information Commissioner; and i) iii) to the extent that it relates to processing of personal data and privacy, any Laws that come into force which amend, supersede or replace existing Laws including the GDPR, the LED and any applicable national implementing Laws as amended from time to time including the DPA 2018 [subject to Royal Assent].
Data Subject	Takes the meaning given in the Data Protection Legislation.
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract 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.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.

Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.10 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.

G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information

	● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier’s or CCS’s possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Direction (Directive (EU) 2016/680).
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed,

	and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	This has the meaning given to it under the Data Protection Act 1998 as amended but, for the purposes of this Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	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: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.

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

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

Schedule 7 - Processing, Personal Data and Data Subjects

DATA PROCESSING ADDENDUM

BACKGROUND:

Where Client is incorporated in any member state of the European Economic Area (“EEA”), Switzerland, or the United Kingdom, or otherwise transfers Personal Data via onward transfer to Diligent (“Diligent”), the following terms in this Data Processing Addendum ("Addendum") shall be incorporated into and form part of the Agreement between Diligent and Client, and, in the event of conflict with any other terms of the Agreement, this Addendum shall prevail. Diligent enters into this Agreement with respect to the Personal Data that is provided by or on behalf of Client. In the event that Data Protection Laws are amended, replaced or repealed, the parties shall negotiate in good faith a solution to enable the transfer of Personal Data to be conducted in compliance with Data Protection Laws.

1. DATA PROTECTION

A Diligent shall act as a Processor when Processing any Platform Data provided to it by Client for the purposes of (i) providing the software-as-a-service subscription purchased by Client under the Agreement, and/or any other services Diligent provides under the Agreement, or (ii) otherwise performing Diligent’s obligations under the Agreement (the “Services”). Where Diligent Processes User Data for the purpose of providing the Services, it shall act as a Processor.

B Diligent agrees that it will, acting as a Processor in the provision of the Services:

(1) Process the Personal Data only for the purpose of providing the Services or as otherwise instructed in writing by Client, and inform Client if any instruction contradicts any legal requirements to which Diligent is subject;

(2) keep all Personal Data confidential as required under the Agreement and ensure that persons authorised by Diligent to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(3) ensure that access to Personal Data shall only be provided to those of its employees, Affiliates or service providers who need access to such data for the performance of the Services for the purposes set out in clause 1.A, and that they will only access Personal Data in order to provide the Services or in accordance with Client's instructions;

(4) take appropriate technical and organizational security measures to safeguard Personal Data against unauthorized access, destruction, disclosure, transfer, or other improper use;

(5) provide Client with access to the Personal Data which have been provided by Client to enable Client to comply with its obligations to Data Subjects exercising their rights under Data Protection Laws. Diligent shall refer such Data Subjects to Client and shall also, at the request of Client, either (i) amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects to ensure that their Personal Data are accurate and complete or (ii) provide the Client with the ability to directly amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects through the Services;

(6) promptly notify Client of any accidental or unauthorized access, destruction, disclosure, transfer or other improper use of Personal Data that have been supplied by Client, after Diligent becomes aware of any such access, destruction, disclosure, transfer or other improper use, or of any complaints by individuals or third parties that involve or pertain to such Personal Data, and shall, taking into account the nature of the Processing and the information available to Diligent, provide such assistance to Client as may be reasonable in the circumstances to enable Client meet its obligations to notify any Supervisory Authority

or any other regulatory or governmental authorities or Data Subjects of such event where Client is required to do so by law;

(7) taking into account the nature of the Processing and the information available to Diligent, assist Client (i) in complying with Client's obligation to implement appropriate technical and organizational security measures; and (ii) in relation to any privacy impact assessments or consultations with Supervisory Authorities about the Processing of Personal Data in the context of the provision of the Services or any inquiry, complaint or claim in relation to the Processing of Personal Data provided by Client;

(8) make available to Client all information necessary to demonstrate that Diligent is in compliance with this clause 1.B;

(9) allow Client to audit Diligent or obtain reasonably reliable documentation regarding the adequacy of the Processing by the Diligent of Personal Data on behalf of the Client. Such documentation may: (i) be an annual SOC1 Type 2 (or subsequent successor) audit of the Diligent's security policies and procedures; (ii) be in accordance with ISO 27001 standards or such alternative standards that are substantially equivalent to ISO 27001; or (iii) otherwise provide for demonstrable assurances of adequacy of the data processing facilities used by the Diligent to Process Personal Data on behalf of the Client ("Audit Report"). If the Client requests in writing, Diligent will provide the Client with a copy of the Audit Report or related documentation so that the Client can reasonably verify the Diligent's compliance with the security obligations under Data Protection Laws. Unless otherwise required by a Supervisory Authority or mutually agreed by the Parties in writing, any audit of Diligent shall be limited to the provision of the Audit Report;

(10) at the termination of the Agreement or this Addendum, at Client's election, delete or return the Personal Data to Client, provided that Client acknowledges and agrees that any Personal Data stored within the software-as-service offerings provided by Diligent to Client shall be deleted either as specified within the Agreement or, if the Agreement is silent, within thirty (30) days of termination of the Agreement;

(11) Client hereby authorizes and consents to the engagement of each of Diligent's Service Providers as subprocessors provided that, at Client's request, Diligent shall make available to Client the current list of Service Providers and their countries of location, as amended from time to time. If Client reasonably believes that any such Service Provider presents an unreasonable risk to Client or prevents Client from complying with Data Privacy Laws, Client may, within thirty (30) days of receiving such notice from Diligent, notify Diligent that it objects to the Service Provider and ask Diligent to provide an alternative Service Provider. If Client so objects, Diligent shall in good faith seek to either (i) provide an alternative Service Provider which addresses Client's objection or (ii) not utilize such Service Provider with respect to the Agreement. If Diligent is unable to do either (i) or (ii), Client shall either withdraw its objection or shall be entitled to terminate the Agreement and this Addendum without cause; and

(12) the selection of a Service Provider under this clause 1.B shall not release Diligent from its responsibility for its obligations under any other applicable agreement Client may have with Diligent and this Addendum. Diligent shall be responsible for the Processing of Personal Data by such Service Provider.

C To the extent that Diligent Processes Personal Data provided to it by Client for purposes other than as set forth in clause 1.A above, Diligent acknowledges that it will be a Controller of that Personal Data, and Diligent agrees to Process such Personal Data in accordance with Data Protection Laws.

D In relation to all Personal Data provided by it to Diligent, Client shall ensure that:

(1) where consent is required, all relevant Data Subjects have consented (in the appropriate manner) to their Personal Data being disclosed to Diligent for Processing in accordance with the Agreement;

(2) the disclosure of Personal Data by Client to Diligent will be in each case and in all respects lawful;

(3) notice of the disclosure of their Personal Data to Diligent for Processing in accordance with the Agreement and this Addendum will be provided to all relevant Data Subjects (including any Users) prior to any such disclosure. If requested by Diligent, Client shall provide evidence that it has provided such notice;

(4) Client complies with, and represents and warrants that it has complied with, the Data Protection Laws in relation to the use of the Services and the performance of the Agreement by Client and its Users;

(5) it shall not, by any act or omission, put Diligent or any of its Affiliates or subsidiaries in breach of any of the Data Protection Laws; and

(6) it shall do and execute, or arrange to be done and executed, each act, document and thing necessary or desirable in order to comply with this clause 1.D.

E Where Client provides Personal Data to Diligent in order for Diligent to provide the Services, Diligent shall Process the Personal Data on Client's behalf. In this case Diligent is a Processor in respect of that Personal Data and in the event that there is a transfer of Personal Data by the Diligent to a sub-processor that is established outside of the EEA, the Diligent shall ensure that such transfer is conducted in accordance with the Data Protection Laws.

F Clauses 1.A, B, and E do not apply where Diligent is acting as a Controller of User Data.

G For the purposes of clauses 1.A, B, C, D, E, and F, only, and for Exhibit 1–2 of this Addendum:

(1) "**Affiliate**" means, with respect to any legally recognizable entity, any other entity Controlling, Controlled by, or under common Control with such entity. “Control” means direct or indirect (i) ownership of more than fifty percent (50%) of the outstanding shares representing the right to vote for members of the board of directors or other managing officers of such entity, or (ii) for an entity that does not have outstanding shares, more than fifty percent (50%) of the ownership interest representing the right to make decisions for such entity. An entity will be deemed an Affiliate only so long as Control exists.

(2) "**Data Exporter**" means Client;

(3) "**Data Importer**" means Diligent;

(4) the terms "**Controller**" "**Processor**", "**Process(ing**)", and "**Personal Data**" each have the meaning given to such terms in the GDPR;

(5) the term "**Data Protection Laws**" means any laws, regulations, or other binding obligations (including any and all legislative and/or regulatory amendments or successors thereto) of the European Union, the EEA, Switzerland, or the United Kingdom that govern or otherwise apply to Personal Data Processed under the Agreement.

(6) the term "**Data Subject**" shall mean an individual who is the subject of Personal Data;

(7) "**Services**" shall have the meaning described in clause 1.A;

(8) "**Service Provider**" means a subprocessor appointed by Diligent to assist with the provision of the Services to the Client or the performance of Diligent's obligations under the Agreement;

(9) the term "**Supervisory Authority**" shall mean the data protection authority in the applicable European state;

(10) the term "**GDPR**" shall mean European Union Regulation 2016/679 and includes any relevant implementing measure in each relevant European state, or any successor legislation thereto;

(11) "**User Data**" means any personal data of Users which is required to provide the Services, such as User ID, User type, name, company affiliation, contact information (business address, phone number, and email address); and

(12) "**User**" means any individual authorized to make use of the Services pursuant to the Agreement.

(13) "**Platform Data**" means all data uploaded by the Client using the software-as-a-service offerings purchased by the Client.

(14) Any capitalized terms not defined in this clause 1.G shall be defined as they are under the Agreement.

2. GOVERNING LAW AND MISCELLANEOUS

This Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed in all respects by, and construed in accordance with the governing law of the Agreement.

Except as otherwise stated herein, this Addendum shall supersede and replace all previous provisions of the Agreement related to Data Protection Laws. Any pre-existing audit rights are superseded by clause 1.B(9) of this Addendum.

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

EXHIBIT 1

Details of the processing activities

This Exhibit forms part of the Addendum.

Data subjects

The European Personal Data concerns the following categories of data subjects (please specify):

The Data Exporter may submit Personal Data to the Data Importer, the extent of which is determined and controlled by the Data Exporter in its discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: Data Exporter's customers, business partners and Diligents of Data Exporter, employees, directors, officers, contact persons, and Users authorized to use the Data Importer services.

Categories of data

The European Personal Data concerns the following categories of data (please specify):

The Data Exporter may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data: Name; home address; photograph; professional email address; professional telephone number (including mobile telephone number); personal email address; personal telephone number (including mobile telephone number); data related to transactions including transactions' purposes; tax ID; government identification number; customer numbers; complaints; bank account details; marketing preferences; IP address; cookie data; login credentials (username and password); traffic data including web logs; images.

Special categories of data (if appropriate)

The European Personal Data concerns the following special categories of data (please specify):

The Data Exporter may, subject to any restrictions set forth in the Agreement, submit special categories of data to the Data Importer, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which is for the sake of clarity is Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation. In any event, any such Personal Data may only be submitted as Platform Data.

Processing operations

The European Personal Data will be subject to the following basic processing activities (please specify):

Processing in the course of performing the Services described in the Agreement.

Duration

The European Personal Data will be Processed by Diligent for the duration of the Services.

EXHIBIT 2

Technical and organisational security measures

This Exhibit forms part of the Agreement.

Description of the technical and organisational security measures implemented and maintained by the Diligent in accordance with clause 1.B(4) (or document/legislation attached):

Data Importer will maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data, including those measures specified in the Agreement.