Department for Education

JAGGAER SOURCE–TO-PAY CONTRACT

Between DfE and Jaggaer

Version Final

February 2019

Crown Commercial Service

G-Cloud 10 Call-Off Contract

This Call-Off Contract for the G-Cloud 10 Framework Agreement (RM1557.10) includes:

Part A - Order Form

Digital Marketplace service ID number:	1566 2481 6608 211
Call-off Contract Reference:	TBC
Call-Off Contract title:	Jaggaer Advantage Source to Pay (S2P)
Call-Off Contract description:	Implementation and supply of Source to Pay E-Sourcing tool
Start date:	18th February 2019
Expiry date:	17th February 2021
Call-Off Contract value:	Fixed Costs of £1,045,025 (ex VAT) Plus optional (non-committed) costs of £350,000 (ex VAT)
Charging method:	As per payment terms with: i) Implementation Services – fixed price ii) Source to Pay tool – fixed price per licence iii) Additional services on an as required basis to be charged in line with the rate card iv) Optional services to be called off by the customer as required
Purchase Order Number	TBC

This Order Form is issued under the G-Cloud 10 Framework Agreement (RM1557.10).

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

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

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

From: the Buyer	**THE SECRETARY OF STATE FOR EDUCATION** whose Head Office is at Sanctuary Buildings, Great Smith Street, London, SW1P 3BT (the "**Buyer**");

To: the Supplier	Jaggaer (trading as BravoSolution UK Limited) 020 7796 4170 Supplier's address: 1st Floor 85 London Wall London EC2M 7AD Company number: 05340218
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: Senior Contract Manager Name: Sherida Kirby Address: Agora Building, Cumberland Place, Nottingham, NG1 6HJ Email: Sherida.Kirby@education.gov.uk Phone: 07990339159
For the Supplier:	Title: Account Director Name: David Sharples Email: dsharples@jaggaer.com Phone: 07825 843903

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 18th February 2019 and is valid for 24 months, until 17th February 2021.
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.
Extension period:	This Call-Off Contract can be extended by the Buyer for two 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 following Cabinet Office approval and 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] [Lot 3 - Cloud support]
G-Cloud services required:	The Services to be provided by the Supplier under Lot 2 Cloud Software are listed in Framework Section 2 and outlined below: The Source to Pay tool as described in "Jaggaer Advantage Source-to-Pay (S2P)"is for up to 500 user licences, although consumption may be increased up to 20% following commercial agreement with Jaggaer. The Source to Pay Suite to include, as and when required:  **£394,000 per year exc. VAT** A breakdown of the licence costs are provided at Schedule 2 and further details of the functionality is provided at Schedule 1
Additional services:	Lot 3 – Cloud Support "Jaggaer Cloud Support Services" Service ID 6325 2668 5273 103 that provides: 

	[redacted] Further details are provided at Schedule 1 **£257,025 exc. VAT**
Location:	The Services will be delivered to any of the Buyers locations as defined in the implementation and adoption services plan. This could include London, Coventry, Sheffield, Manchester or Darlington or at the suppliers premises.
Quality standards:	Jaggaer will provide the services to the agreed quality standards within the G-Cloud framework.
Technical standards:	The technical standards required for this Call Off contract are: 1) System security, availability and reliability maintained to ISO270001/20000-1/22301/27018 standards 2) Data to be hosted only within the United Kingdom or European Economic Area 3) Tool to remain compatible with current Microsoft software and Internet Browsers) 4) Cyber Essentials accreditation 5) Compliance with accessibility standards W3C WA1: WCAG 2.0 AA level
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as defined in the Service Level Agreement available to download at: https://www.jaggaer.com/terms-of-service/saas-applications-support-services-terms/ and also contained at Schedule 9 The KPI's agreed for this Service are as follows: • Service Availability @ 99.5% per calendar month. (Service credits apply for service >99.5% - details within Schedule 9) • Response to Severity Levels

	<table><tr><td></td><td>Initial response</td><td>Deliver of Situation</td></tr><tr><td>Level 1 (Urgent)</td><td>1 hr</td><td>8 hrs</td></tr><tr><td>Level 2 (High)</td><td>4 hrs</td><td>2 business days</td></tr><tr><td>Level 3 (medium)</td><td>1 business day</td><td>3 business days</td></tr><tr><td>Level 4 (Low)</td><td>2 business days</td><td>5 business days</td></tr></table> - Implementation Plan is delivered to quality and time and signed off as meeting full requirements - Change Requests are actioned and implemented by deadlines agreed - Training provided is delivered to time and quality standards agreed
Onboarding:	The Buyer and Supplier shall attend a start-up meeting with representatives of the Buyer (date to be agreed between Buyer and Supplier.) At this meeting the agenda will include but not be limited to: discussion and agreement on activity to implement the service within the DfE, future contract management arrangements; project documentation and deliverables; service delivery KPIs; requirements for reporting of Management Information consistent with clause 8 of the framework agreement (if any); and a forward schedule of meeting dates. As a minimum, the Supplier's Account Manager for the DfE shall attend and fully participate in agreed contract and service review meetings chaired by the Buyer. The agenda for this meeting will be issued to participants at least three (3) working days in advance of the meeting and include a monthly Service Report produced by the Supplier. Frequency of meetings will be monthly, with the potential to increase should the service degrade / risk increase. The detailed content of the Service report shall include as a minimum: progress against delivery of all work packages, forward and retrospective resource plan, risks and issues log, financial reporting, incidents and service failure log; quality assurance.

Offboarding:	The offboarding plan for this Call-Off Contract is BravoSolution can provide a data extract at the cost of £3,000 (ex VAT). If requested, BravoSolution would proceed, within thirty-five (35) working days from the Buyer Access In Read-Only mode Date or, if not defined, from the Agreed Closing Date, to the extraction of Client Data entered on or managed by the Portal/Platform, in the following standard format produced by the standard BravoSolution data extract procedure: a) All extracted data will be saved in documents and files organised for browsing in a folder – sub-folders structure (for instance, by Project and by RFQ) b) All data entered through forms and all reports shall be rendered as summary into pdf (portable document format) files; c) All files attachments shall be extracted in their original format; d) Supplier identification data and some listed information shall be extracted in MS Excel format The data shall be copied on a storage unit such as a Hard Disk or DVD, according to volume and returned to the Client. Read only access to and maintenance of a legacy portal may be provided at a cost of £5,000 per year for audit purposes if required This is an additional charge that has not been included in any of the costs provided elsewhere.
Collaboration agreement:	The Buyer does not require the Supplier to enter into a Collaboration Agreement.
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed £1,000,000. The annual total liability for Buyer Data defaults will not exceed £1,000,00 or 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other defaults will not exceed the greater of £1,000,000 or 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
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 or any higher limit the Buyer requires (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 60 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. As agreed with the Supplier.
Buyer's responsibilities:	The Buyer is responsible for providing prompt access to relevant stakeholders for kick-off workshop / implementation consultation sessions, timely provision of templates for import, suitable provision of training facilities including PCs with internet connect, projector, whiteboard, etc.
Buyer's equipment:	In order to access the service, the Buyer must be equipped with computer with internet connection and internet browser (e.g. Internet Explorer, Firefox, Chrome).

Supplier's information

Subcontractors or partners:	The following is a list of the Supplier's Subcontractors or Partners: [There are no Subcontractors/Partners associated with this agreement.]

Call-Off Contract charges and payment

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

Payment method:	The payment method for this Call-Off Contract is BACS.
Payment profile:	The payment profile for this Call-Off Contract is

	Technology licences annually in advance, first payment due on contract signature.  If there is any discrepancy with the delivery of the outputs expected prior to the 1st and/or 2nd milestone date (be that in the level of quality or deadlines agreed) that are not related to actions unfulfilled by the Buyer then the Buyer will refrain from paying the next milestone charge until the discrepancy has been resolved. Any additional consultancy days called off will be paid monthly in arrears when based on the Ad Hoc rate.
Invoice details:	The Supplier will issue electronic/paper invoices as per the payment profile above. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Electronic invoices will be sent to: APinvoices-DFE-U@sscl.gse.gov.uk
Invoice information required - for example purchase order, project reference:	A valid invoice is one that is: • Is in an un-editable format such as pdf or jpeg • Delivered in timing in accordance of the contract and is not future dated • Is for the correct sum • Is correct in terms of services/goods supplied • Has a unique invoice number • Quotes a valid Purchase Order number • Includes correct supplier details, date, contact details • Valid Contract Number Invoicing will be in £ Sterling A copy invoice shall simultaneously be emailed to the DfE Buyer to enable the Buyer to take receipting action.

Invoice frequency:	Invoice will be sent to the Buyer in accordance with the above payment schedule.
Call-Off Contract value:	The total value of this Call-Off Contract is fixed costs of £1,045,025 (ex VAT) Plus optional (non-committed) costs of £350,000 (ex VAT)
Call-Off Contract charges:	The breakdown of the Charges is;  Further details are provided at Schedule 2 Call Off Charges. In addition to the above the Supplier shall work with the Buyer to minimise the impact on the public purse of T&S associated with the operation of this contract. Unless otherwise provided for under the Supplier's G-Cloud 10 framework offering and/or the Supplier has an office in close proximity of the Buyers office where a meeting is to be held (approx. 25 miles radius), where expenditure on T&S is identified as being necessary for the effective operation of the contract, T&S will be paid at the level commensurate with the Buyer rate in place at the time the expenditure is incurred. DfE rates in place as at 1st Jan 2019 are listed below: • Hotel accommodation bed and breakfast – London £110.00 including VAT and elsewhere £75.00 including VAT • Rail travel shall be restricted to standard class • Car mileage at the 'Public Transport Rate' of 0.25p per mile • Taxis only payable where their use can be justified against using public transport No other out of pocket expenses shall be allowable.

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following implementation plan, exit and off-boarding plans and milestones as per the accepted proposal.
Guarantee:	The Buyer does not require a Guarantee from the Supplier.
Warranties, representations:	In addition to the incorporated Framework Agreement clause 4.1, Supplier's warranties and disclaimer of warranties shall be as set forth in Section 6 of Supplier's Master Subscription Agreement Terms and Conditions, United Kingdom version 19 March 2018, available at https://www.jaggaer.com/msa/gb/v13072018/, which is incorporated herein by reference.
Supplemental requirements in addition to the Call-Off terms:	Not applicable.
Alternative clauses:	Not applicable.
Buyer specific amendments to/refinements of the Call-Off Contract terms:	Within the scope of the Call-Off Contract, the Supplier will also agree to additional terms detailed at Schedule 8.
Public Services Network (PSN):	Not applicable
Personal Data and Data Subjects:	Schedule 7 - Processing, Personal Data and Data Subjects does apply

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 RM1557.10.

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

Signed:	**Supplier**	**Buyer**
Name:	Richard Hogg	Susan Dawson

Title:	Managing Director, UK & Ireland	Deputy Director, DfE Commercial
Signature:		
Date:	15th February 2019	

Schedule 1 - Services

A) Lot 3 Cloud Software – Source to Pay Toolset and Award Toolset

The Supplier shall provide Lot 3 Cloud Software in accordance with the service definition " Jaggaer Advantage Source-to-Pay (S2P) – Service ID 1566 2481 6608 211 of the Digital Market Place. The Supplier will deliver a commercial off-the-shelf (COTS), web based, fully hosted and managed, software-as-a-service (SaaS) solution to the Buyer.

The modules will be used as follows:

INCLUDED:

[redacted]

OPTIONAL

[redacted]

NOT INCLUDED:

[redacted]

The environments monitored under the SaaS solution are:

- **Pre-preparation environment (PREP).** This is System architecture used for the provison of BravoSolution Advantage S2P releases or new features/contents for

review and approval from the Buyer. Each configuration modification (e.g. parameters and settings) to the system configuration will be presented by the Supplier on the PREP environment in advance of release on the Production (PROD) site (unless it is a critical security patch in which case both sites will be updated in parallel) and so the most recent configurations will be present on PREP when modelling any new release functionality. In this way, PREP is effectively used for staging, verifying and validation applications before on line release. On request, this environment can also be used by the Buyer as a test and training instance of the application soon to be deployed in the Production environment. In case of major change in the application, adequate time should be reserved for testing and training prior to launch.

- **Production environment (PROD).** This is System architecture used by BravoSolution Advantage S2P Clients (Buyer and Vendors) as a "real" environment to access the range of modules and active features.

Further details on each module is available within the Service Definition document from GCloud. Links below to this document, the rate card and Supplier's T&C.s

Also attached is the Supplier's response to the Buyers Functional Requirements. An initial assessment of the requirements against the Service ID documentation was undertaken by the Buyer and the document below identifies the gaps which was issued to the Supplier for response.

B) Implementation Services

The Supplier shall provide to the Buyer Additional Services to both implement the Source-to-Pay toolset in accordance with the service definition " Jaggaer Cloud Support Services" Service ID 6325 2668 5273 103

[redacted]

[redacted]

A Solution Design Document (SDD) documenting all of the Buyers decisions and configuration preferences agreed during the implementation workshops shall be produced by the Supplier. This SDD shall be presented to the Buyer prior to building/applying any configurations/data into the Buyers PREP environment.

Buyer User Acceptance Testing (UAT) shall be conducted on the Buyers PREP environment prior to the PROD environment being configured.

Further details on these Implementation Services are available within the Service Definition document from GCloud. Links below to this document, the rate card and Supplier's T&C.s are above. Copy of the GCloud entry for the Support Services is below:

JAGGAER Cloud Support Services - D

C) Training

The Supplier shall provide (based on agreed rates and sign off) a blended range of training materials/events designed to provide education and assessments to the end users at the time these services are needed. These include but are not limited to:

[redacted]

A train the Trainer programme shall be made available on request.

Further details are provided within the Service Definition document attached above.

D) User Support Helpdesk

In support of the Jaggaer Advantage suite, the Supplier shall provide a reactive technical and functional issue resolution support associated to the Advantage software solution. The standard support is for:

- Suppliers and all licensed Supplier Management
- Sourcing
- Contract Lifecycle Management, and
- Super/admin users.

It excludes additional services such as Auction Monitoring, Vendor Scouting and Registration.
The support service can be upgraded to cover the entire user community and the excluded services above if required.

The Support is available, as a minimum, from 08:00 to 18:00 UK time excluding Public Holidays. It will operate a level 1, level 2 and level 3 support and availability via phone, email and 'call-me-back' facility

Further details are available within the Service Definition document attached above and SLA's are contained within Schedule 9 .

E) BAU Consultancy Days

The Supplier shall provide Business as Usual or Early Life Support days to the buyer to assist with user adoption or any change requests required following initial configuration. Following the usage of the 30 days contained in the contract the Supplier will provide additional days following sign off from the buyer and charged at the agreed rates in the rate card.

Schedule 2 - Call-Off Contract charges

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

Cloud Software – Source to Pay toolset

The charges for usage of the Source-to-Pay toolset is £394,000 per annum (exc VAT). This includes:

[redacted]

Licence volumes are contained within the attached cost model :

DfE Cost Breakdown to discu

Implementation Services

The implementation Services shall be charged on the basis of the following milestone Charges:

Ref	Milestone	Charge	Acceptance criteria
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]

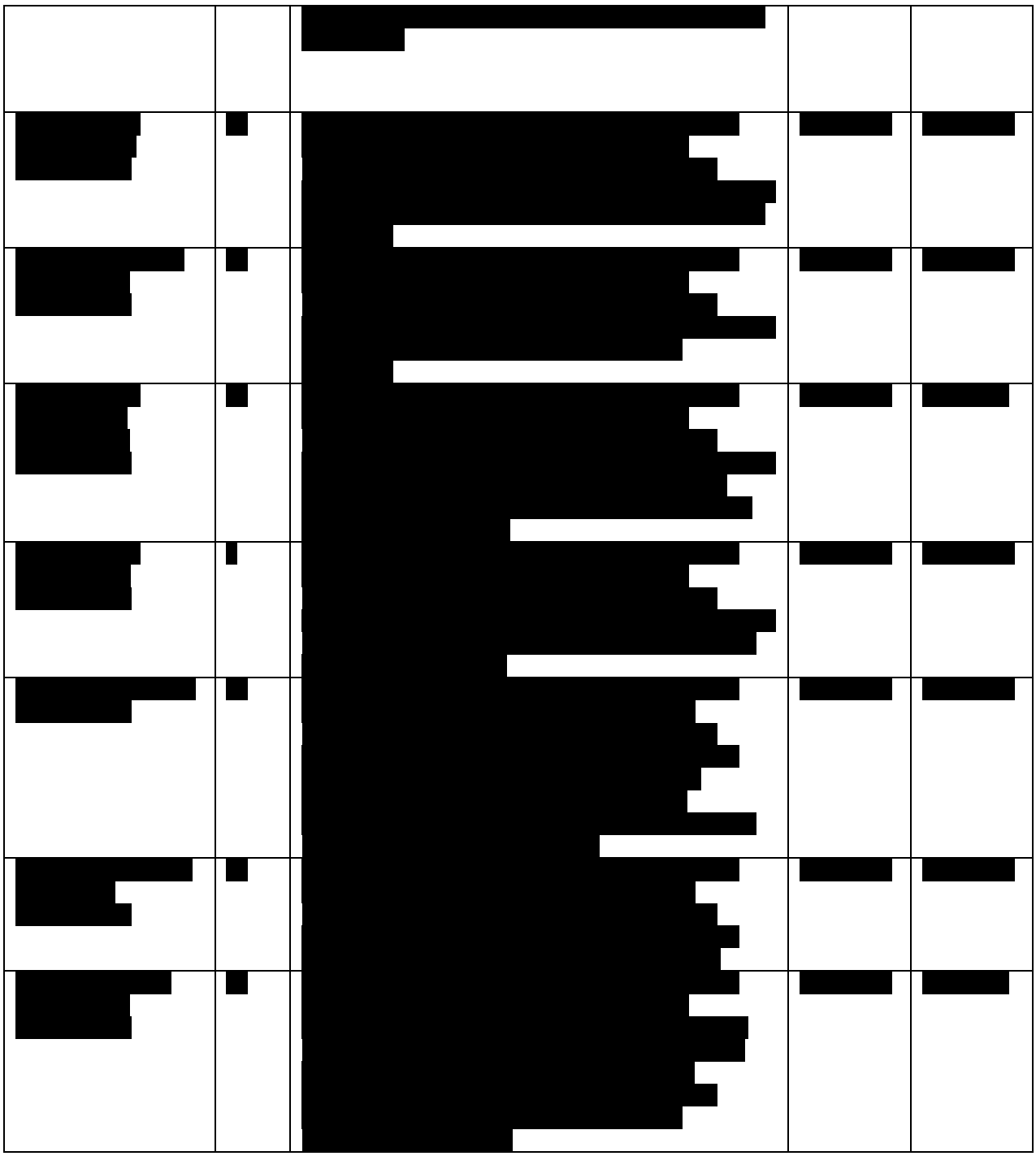
3	[redacted]	[redacted]	[redacted]

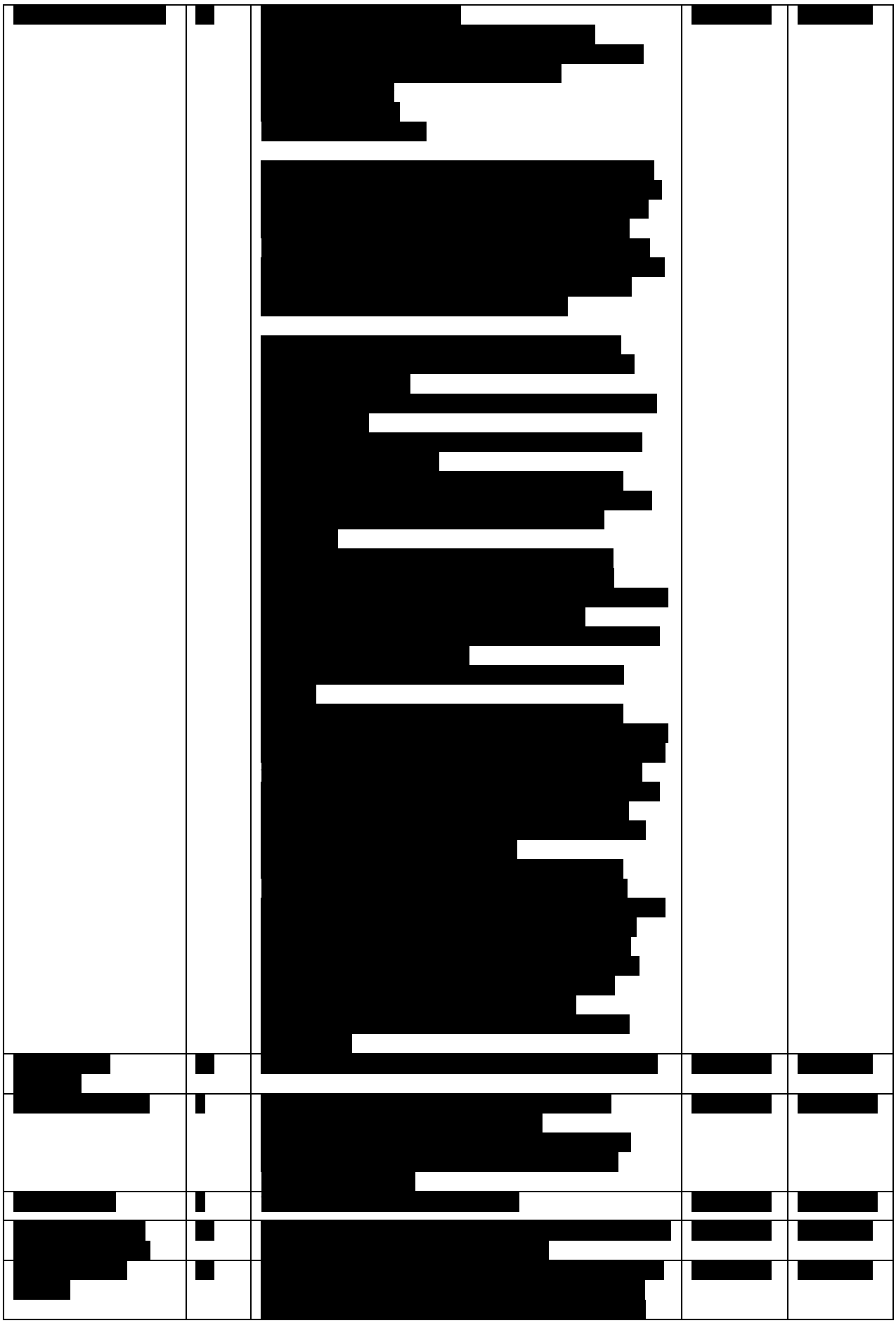
Implementation

The table below provides the breakdown of the activities and the no of days required to implement the modules listed above. This is based on a fixed cost.

The Supplier will create a project management log in an online tool (Smartsheet) that will contain the project plan as well as a RAID log with actions assigned to members of the project team. This will be used for monitoring purposes by both the Supplier and the Buyer.

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





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

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

Options – Included to allow DfE to build contingency into the budget, not included in contract value from start date

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

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

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)
- 5.2 to 5.3 (Force majeure)
- 5.6 (Continuing rights)
- 5.7 to 5.9 (Change of control)
- 5.10 (Fraud)
- 5.11 (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 Legislation 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. 18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 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 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 assist the Buyer with the preparation of any Data Protection Impact Assessment required by the Data Protection Legislation 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, details of which shall be provided to the Buyer on request, 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
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 Union unless the prior written consent of the Buyer has been obtained, which shall be dependent on such a transfer satisfying relevant Data Protection Legislation requirements.

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 without undue delay 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, and insofar as this is possible, 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.

33.9 Before allowing any Sub-processor to Process any Personal Data related to this Framework Agreement, the Supplier must:

i) notify the Buyer in writing of the proposed Sub-processor(s) and obtain its written consent;
ii) ensure that it has entered into a written agreement with the Sub-processor(s) which gives effect to obligations set out in this Clause 33 such that they apply to the Sub-processor(s); and
iii) inform the Buyer of any additions to, or replacements of the notified Sub-processors and the Buyer shall either i) provide its written consent or ii) object.

33.10 The Buyer may at any time put forward a Variation request amend this Call-Off Contract 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, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: • 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	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
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) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; iii) all applicable Law about the processing of personal data and privacy.
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	A claim as set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how

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

	transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	Takes the meaning given in the Data Protection Legislation 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

Glossary:

For the purposes of this Schedule 7, these terms shall be defined as follows:

"Supplier" or "JAGGAER" shall mean SciQuest, Inc., dba JAGGAER
"Buyer" shall mean Department of Education
"Vendor" shall mean an individual or entity with whom Buyer interacts via the Solution
The "Solution" shall mean the JAGGAER Applications, specifically the Source to Pay Solution Buyer is purchasing a subscription to under this Agreement.
"Authorized Users" shall mean (i) Buyer's employees, contractors, subcontractors and outsourcing Vendors, in each case who have been supplied user identification and passwords by Buyer.
"Business Contacts" shall mean Buyer's business contacts within the JAGGAER Applications who are natural persons (for example, a third party whose information is contained in a contract document or other attachment).

Subject matter of the processing:

The processing is needed in order to ensure that the Processor can effectively deliver the contract and provide a Source to Pay solution (this excludes eProcurement and Accounts Payable functionality) (the "Solution"). The Solution allows Suppliers to on-board their details (these fields are pre-defined by the system) and these are, in turn, used by Buyer for sourcing, contract management and category management activities.

Duration of the processing:

The duration of processing will be in alignment with the contract start and end dates.

Nature and purposes of the Processing:

Supplier's purpose of processing is to provide the Solution in accordance with this Agreement. The nature of the processing is any operations necessary to provide the aforementioned Solution. The Buyer's purpose of the processing, through use of the Solution, is to capture the full end-to-end process involved with any commercial activity. This is from the inception of an "idea" or a business need to the collation and storage of all of the documentation and approvals needed. The Solution will allow access to a Supplier's details held on the system and this will be used to run the Sourcing activity. This includes the issuing of an ITT, dealing with correspondence to and from suppliers, evaluation of tenders, generation of award reports and creation of the contract. Alongside this, information on a supplier's performance during the life of a contract will be collated and stored for contract management purposes. Spend information linked to each Supplier will be collated and stored in the system to allow for category management activities.

Type of Personal Data:

The categories of Personal Data processed are determined and controlled in the sole discretion of the Buyer pursuant to the Agreement.

The Personal Data processed includes:

I. Professional Contact Information of Authorized Users and Business Contacts:
- Name and Surname
- Title and position

- Name of Company
- Business email address
- Business physical address
- Business phone number

II. Data derived from use of the JAGGAER Applications including:
- Log-in credentials: user name and passwords
- Log-in and connection data

III. Business transaction* data processed within the JAGGAER Applications which may contain Personal Data if Buyer's current or potential customers and Vendors exported into the JAGGAER Applications are natural persons, such as:
- Contractual relationships with current and potential vendors and customers
- Tax ID Number for Buyer or a Vendor as a natural person
- Purchase Data
- Bid Submissions
- Business credit cards issued under a personal name

** this information may be included in tender documents or contract documents*

Categories of Data Subject:

The Personal Data processed concern the following categories of data subjects:

1. Users of the JAGGAER Applications which includes:
   - Employees (perm and temp) and contractors of Buyer
   - Any other Authorized Users accessing the Solution under Buyer's Subscription

2. Buyer's Business Contacts within the Solution including:
   - Buyer's current and potential customers and related Authorized Users
   - Buyer's current and potential business partners and related and related Authorized Users

Note: In regard to some information uploaded by a Vendor or included in a Vendor's response to a request for information that is Processed in the Solution, the Vendor uploading the information may be the "controller" of that data and Buyer the "processor." In such circumstances, Buyer is still the "controller" relative to JAGGAER and JAGGAER is processing the data on Buyer's behalf.

Plan for return or destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data:

Data will be retained for the duration of the contract. Along with the deactivation of the BA instance the Buyer can request the extraction of the exportable data stored within its JaggaerAdvantage instance, as detailed in Off-boarding section of the Order Form. Further details around the service and data removal process will be established at the end of the contract. Following the data extraction, if requested, all customer data will be destroyed once the data extraction has been successfully transferred. This will be completed within 30 working days.
The operational processes to manage the execution of services removal and the destroying of data are described in JAGGAER documented security procedures. Documented embedded below.

Further details regarding processing of data shall be as set forth in the Data Processing Addendum, which shall be executed by the parties prior to implementation of the Solution and is hereby incorporated by reference.

JAGGAER Technical and Organizational

Schedule 8 – Additional Buyers Terms and Conditions

Additional Terms and Conditions for Inclusion in the G-Cloud Contract

In addition to the G-Cloud framework and Call Off Terms and Conditions the following clauses shall apply. They will be included within the Call Off Order Form and therefore apply according to the order of precedence detailed at CO-1.2 of the Call Off Terms and Conditions.

1. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	a level of security clearance described as pre-employment checks in the National Vetting Policy. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" "Certified Cyber Security Consultancy"	is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-professional
"CC" "Common Criteria"	the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.
"CPA" "Commercial Product Assurance" [formerly called "CESG Product Assurance"]	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.

	There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: https://www.iasme.co.uk/apply-for-self-assessment/
“Data” “Data Controller” “Data Processor” “Personal Data” “Sensitive Personal Data” “Data Subject”, “Process” and “Processing”	shall have the meanings given to those terms by the Data Protection Act 2018
"Department’s Data" “Department’s Information”	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
“DfE” “Department”	means the Department for Education
“Departmental Security Standards”	means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
“Digital Marketplace / GCloud”	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.
“FIPS 140-2”	this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled ‘Security Requirements for Cryptographic Modules’. This document is the de facto security standard used for the accreditation of cryptographic modules.
“Good Industry Practice” “Industry Good Practice”	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.

“Good Industry Standard” “Industry Good Standard”	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“GSC” “GSCP”	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
“HMG”	means Her Majesty’s Government
“ICT”	means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	The National Cyber Security Centre (NCSC) formerly CESG is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
“OFFICIAL” “OFFICIAL-SENSITIVE”	the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services. the ‘OFFICIAL–SENSITIVE’ caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.

“Secure Sanitisation”	Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable. Secure sanitisation was previously covered by “Information Assurance Standard No. 5 - Secure Sanitisation” (“IS5”) issued by the former CESG. Guidance can now be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
“Security and Information Risk Advisor” “CCP SIRA” “SIRA”	the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
“SPF” “HMG Security Policy Framework”	This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework
”Tailored Assurance” [formerly called “CTAS”, or, ”CESG Tailored Assurance”]	is an ‘information assurance scheme’ which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology

1.1. The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

1.2. Where the Contractor will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme”. The certification scope must be relevant to the services supplied to, or on behalf of, the Department.

1.3 The Contractor shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

1.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

1.5 Departmental Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Contractor and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.

1.6 The Contractor shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas

1.7 The Contractor shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.

1.8 (The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.

1.9 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which has been certified to FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.

1.10 Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.11 and 1.12 below.

1.11 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.

1.12 (All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.

1.13 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

1.14 When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

1.15 At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Contractor's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

1.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.

1.17 (All Contractor or sub-contractor employees who handle Departmental Data The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

1.18 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, or any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution, shall be investigated immediately and escalated to the Department by a method agreed by both parties.

1.19 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

1.20 The Contractor or sub-contractors providing the service will provide the Department with full details of any storage of Departmental Data outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Contractor or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department.

1.21 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors, compliance with the clauses contained in this Section.

1.22 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

1.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA)

1.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:

- Existing security assurance for the services to be delivered, such as: PSN Compliance as a PSN Customer and/or as a PSN Service; NCSC (formerly CESG) Tailored Assurance (CTAS); inclusion in the Common Criteria (CC) or Commercial Product Assurance Schemes (CPA); ISO/IEC 27001 / 27002 or an equivalent industry level certification. Documented evidence of any existing security assurance or certification shall be required.
- Existing HMG security accreditations or assurance that are still valid including: details of the body awarding the accreditation; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement. Documented evidence of any existing security accreditation shall be required.
- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

Schedule 9 – Jaggaer's Terms of Service and Service Level Agreement (detailed at "Service level agreement" in Order Form)

Support Services for the JAGGAER Indirect Software-as-a-Service ("SaaS") Applications and JAGGAER Advantage (formerly, BravoSolution) SaaS Applications

1. **ATTENTION! THE FOLLOWING SUPPORT SERVICES TERMS WILL BE LEGALLY BINDING ON CLIENT UPON EXECUTION OF AN AGREEMENT WITH JAGGAER FOR ANY JAGGAER INDIRECT OR JAGGAER ADVANTAGE SAAS APPLICATIONS. CLIENT SHOULD CAREFULLY READ THE FOLLOWING SUPPORT SERVICES TERMS BEFORE EXECUTING THE AGREEMENT.**
2. **Support Services Hours; Contact Information.** Hours and contact information for the maintenance and support services ("Support Services") are listed below.

JAGGAER Applications	Support Hours	Support Contact Information
JAGGAER Indirect: eProcurement and AP Applications	**Clients**: 4:00 a.m. ET Monday – 8:00 p.m. ET Friday, excluding JAGGAER U.S. holidays (which shall be communicated by JAGGAER to Client reasonably in advance), and 24×7 access for reporting Severity Level 1 Incidents (as defined below) **Suppliers**: 12:00 a.m. ET Monday –	• +1-800-233-1121 (Global) • JAGGAER's Support Services web portal at https://www.jaggaer.com/service-support/jaggaer-solutions-portal/

JAGGAER Applications	Support Hours	Support Contact Information
	11:59 p.m. ET Friday, excluding JAGGAER U.S. holidays	
JAGGAER Indirect: Spend Radar Application	**Clients**: 8:00 a.m. ET Monday – 5:00 p.m. ET Friday, excluding JAGGAER U.S. holidays	• Email: support@spendradar.com
JAGGAER Indirect: Advanced Sourcing Optimizer, Total Supplier Manager and Sourcing Director Applications	**Clients**: 12:00 a.m. ET Monday – 11:59 p.m. ET Friday, excluding JAGGAER U.S. holidays (which shall be communicated by JAGGAER to Client reasonably in advance), and 24×7 access for reporting Severity Level 1 Incidents (as defined below) **Suppliers**: 12:00 a.m. ET Monday – 11:59 p.m. ET Friday, excluding JAGGAER U.S. holidays	• +1-800-233-1121 (Global) • JAGGAER's Support Services web portal at https://www.jaggaer.com/service-support/jaggaer-solutions-portal/

JAGGAER Applications	Support Hours	Support Contact Information
JAGGAER Advantage Applications	**Clients**: 12:00 a.m. GMT Monday – 11:59 p.m. GMT Friday, and 24×7 access for reporting Severity Level 1 Incidents (as defined below)	• 877-528-2947 (U.S.) • Email: customersupport@bravosolution.com • Live Chat; enabled upon Customer request • + [International Access Code] 800 2255 4626. Universal International Free Number (UIFN) dialing plan is located at: https://www.bravosolution.com/uifn/

3. **Support Contacts**. Except for the Advanced Sourcing Optimizer Application, JAGGAER shall provide Support Services for to up to three (3) designated, authorized, qualified and trained users of the JAGGAER Applications ("Support Contacts") free of charge. Additional Support Contacts may be available, subject to additional fees (Discuss with your account manager). In addition to being authorized to request Support Services from JAGGAER, Support Contacts act as the Client's point of contact for JAGGAER Support Services notifications, including maintenance windows, Service Level Availability alerts and security-related matters. For JAGGAER's Total Supplier Manager, Sourcing Director and eProcurement Applications, Support Services for Client's suppliers shall be limited to technical assistance and shall not include Client supplier questions related to Client's business or operations. There are no restrictions on the number of users of the Advanced Sourcing Optimizer Application that may request Support Services.

4. **Response Times**. JAGGAER will use commercially reasonably efforts to provide Support Services in accordance with the response times shown in the table below. Determination of severity levels shall be within JAGGAER's sole discretion, acting reasonably.

Severity Level	Initial Response	Delivery of a Solution or Action Plan
Severity Level 1 (Urgent): An Incident that severely impacts your use of the JAGGAER Application for production purposes (such as loss of production data or your production systems are not functioning). The Incident halts your business operations and no procedural work around exists.	**1 Hour**	**8 Hours**
Severity Level 2 (High): An Incident where the JAGGAER Application is functioning but your use for production purposes is severely reduced. For	**4 Hours**	**2 Business Days**

Severity Level	Initial Response	Delivery of a Solution or Action Plan
production purposes where the Incident is causing a high impact to portions of your business operations and no procedural work around exists.		
Severity Level 3 (Medium): An Incident that involves partial, non-critical loss of use of the JAGGAER Applications for production purposes. For production purposes, there is a medium-to-low impact on your business, but your business continues to function.	**1 Business Day**	**3 Business Days**
Severity Level 4 (Low): A general usage question, reporting of a documentation error or recommendation for a future product enhancement or modification. For production purposes, there is low-to-no impact on your business or the performance or functionality of the JAGGAER Applications.	**2 Business Days**	**5 Business Days**

5. **Service Level Availability**. JAGGAER shall make all JAGGAER SaaS Applications available to Client for at least ninety-nine and one half percent (99.5%) of the time (determined monthly on a calendar basis), seven (7) days a week, twenty-four (24) hours per day, not including any unavailability that (i) results from JAGGAER maintenance communicated in advance or (ii) results from the poor performance or, of failure of, internet service or other outside service, software or equipment not within the control of JAGGAER ("Service Level Availability"). JAGGAER test and pre-production environments are expressly excluded from this or any other service level commitment.
6. **Service Level Availability Reporting for the JAGGAER Indirect Applications**. Real-time and historic Service Level Availability for the JAGGAER Indirect Applications may be viewed at https://www.jaggaer.com/service-support/uptime-report/
7. **Service Level Availability Commitment.** JAGGAER commits to provide the Service Level Availability set forth above. If in any calendar month this Service Level Availability commitment is not met by JAGGAER and Client was negatively impacted (i.e., attempted to log into or access the JAGGAER Applications and failed due to the unscheduled downtime of the JAGGAER Applications), JAGGAER shall provide, as Client's sole and exclusive remedy, a service credit calculated as set forth below:
    a. If Service Level Availability is greater than 99% and less than 99.5%, the service credit shall be 5% x 1/12th of the annual Subscription Fee for those JAGGAER Applications that were actually negatively impacted; and

b. If Service Level Availability is greater than 98% and less than 99%, the service credit shall be 10% x 1/12th of the annual Subscription Fee for those JAGGAER Applications that were actually negatively impacted; and
c. If Service Level Availability is less than 98%, the service credit shall be 15% x 1/12th of the annual Subscription Fee for those JAGGAER Applications that were actually negatively impacted.

8. **Credit Request**. In order to receive a credit under this Service Level Availability commitment, Client must request it by emailing JAGGAER at SLA@JAGGAER.com within seven (7) business days of the end of the applicable month. If Client submits a service credit request and does not receive a prompt automated response indicating that the request was received, Client must resubmit the request because the submission was not properly received and will not result in a credit. Clients who are past due or in default with respect to any payment or any material contractual obligations to JAGGAER are not eligible for any credit under this Service Level Availability commitment. JAGGAER shall calculate any service level downtime using JAGGAER's system logs and other records. JAGGAER shall issue the service credit against the next invoice and if there is no future invoice, a service credit will be provided in the form of a refund.
9. **Client Support Expectations.** Client will maintain and manage internal support capabilities to address end-user inquiries through Client's or Client's subcontractor's Support Contacts within Client's (or Client's subcontractor's) organization and determine whether an issue or defect ("Incident") should be communicated to JAGGAER by a Support Contact for Support Services (e.g. a help desk). The Support Contact shall conduct reasonable and adequate research with respect to an Incident prior to contacting JAGGAER for assistance. Client shall use commercially reasonable efforts to assist JAGGAER in reproducing the specific situation in which a JAGGAER Application, standing alone, demonstrates a failure to substantially conform to all published, functional and technical specifications for the applicable version of the JAGGAER Applications (the "Specifications"). JAGGAER will use commercially reasonable efforts to correct reproducible errors to enable the JAGGAER Application to perform substantially in accordance with the Specifications.
10. **Incident Tracking for the JAGGAER Indirect Applications**. For the JAGGAER Indirect Applications, reported Incidents shall be reported, logged, and tracked via the use of an incident tracking system, which system may be accessed via accessing a web site. Upon notification by Client of an Incident via the web-tracking tool, an Incident Tracking Number ("ITN") shall be assigned which will remain open until the Incident is resolved or Client becomes non-responsive. Client must refer to said ITN for all subsequent inquiries with regard to the Incident.
11. **Updates**. JAGGAER may from time to time provide new feature functionality, enhancements, and other changes, which are logical improvements to a JAGGAER Application and which JAGGAER elects to make available to all JAGGAER clients on a commercial basis in the form of a release or otherwise ("Updates"). Updates do not include any new software products that

are then made generally available on a commercial basis as separate, price-listed options or additions to a JAGGAER Application nor do they include any Professional Services that may be required for implementation.

12. **Scope of Support Services**. When a JAGGAER Application is deployed in conjunction with other software products, including but not limited to web servers, databases, and operating systems, JAGGAER is not responsible for providing Support Services for these other products, or for ensuring correct interoperation with these products. Client is responsible for ensuring it is using JAGGAER's recommended browsers when using the JAGGAER Applications and JAGGAER is not responsible for providing Support Services related to browsers not recommended by JAGGAER. At Client's request, JAGGAER may provide technical, operational or other assistance or consulting in excess of the standard Support Services described herein for additional fees under the terms of a Statement of Work executed by JAGGAER and Client. Support Services do not include any on-site services and JAGGAER shall be reimbursed by Client for any reasonable travel and living expenses and travel time, to be invoiced by JAGGAER on a monthly basis.
13. **Exclusions.** The Support Services exclude any services required to resolve any Incidents arising from or related to: (i) use of the JAGGAER Applications not in accordance with the Agreement, including applicable Specifications; (ii) modification by Client or any third party of any part of the JAGGAER Applications or interface software that interacts with the JAGGAER Applications; (iii) alteration of any underlying data or data structure of, or related to, the JAGGAER Applications other than through use of the JAGGAER Applications in accordance with the Agreement, including the applicable Specifications; (iv) making changes to site configuration as finalized upon Solution Acceptance during implementation and (v) third party software. Any Professional Services provided by JAGGAER to correct any Incidents arising from or related to the items above shall be subject to additional fees under the terms of a Statement of Work executed by JAGGAER and Client. At Client's request, JAGGAER may provide technical, operational or other assistance or consulting in excess of the standard Support Services on a fixed-price basis under a Statement of Work mutually agreed upon by JAGGAER and Client or in connection with a Premium Support Services offering that may be available. Contact your account manager regarding availability and pricing for Premium Support Services.
14. **Premium Support Services**. Support Services outside of standard Support Services may be available for additional fees in accordance with a Statement of Work executed by JAGGAER and Client, or as a JAGGAER Premium Support offering, if available. Contact your account manager regarding availability and pricing for Premium Support Services.