

G-Cloud 9 Call-Off Contract

This Call-Off Contract for the G-Cloud 9 Framework Agreement (RM1557ix) includes:

[**Part A - Order Form** 2](#_Toc60414)

[**Schedule 1 - Services** 6](#_Toc60415)

[**Schedule 2 - Call-Off Contract charges** 7](#_Toc60416)

[**Part B - Terms and conditions** 7](#_Toc60417)

[**Schedule 3 - Collaboration agreement** 21](#_Toc60418)

[**Schedule 4 - Alternative clauses** 21](#_Toc60419)

[**Schedule 5 - Guarantee** 21](#_Toc60420)

[**Schedule 6 - Glossary and interpretations** 21](#_Toc60421)

# Part A - Order Form

**Digital Marketplace service ID number:**

642182005104408

**Call-Off Contract reference:**

ICT2017/238

**Call-Off Contract title:**

Splunk Enterprise Security (SIEM)

**Call-Off Contract description:**

Splunk Enterprise Security is a SIEM that provides

insight into machine data generated from security

technologies such as network, endpoint, access,

malware, vulnerability and identity information. It enables

security teams to quickly detect and respond to cyber

attacks to simplify threat management while minimizing

risk and safeguarding your business

**Start date:**

20

/02/

18

**Expiry date:**

Initially 12 months to 19/02/2019. (Plus potential extensions

described in “Call off Contract term” section below)

**Call-Off Contract value:**

£93,100.00 excluding VAT

**Charging method:**

Payment will be made within 30 days of the date of the invoice

by BACS

**Purchase order number:**

TBA

his Order Form is issued under the G-Cloud 9 Framework Agreement (RM1557ix).

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**

Department for Education,

Earlsdon Park,

Coventry,

Warwickshire, CV1 3BH

The Secretary of State for Education

This contract is available for use by the DfE, its Executive Agencies and across the DfE family

and partner organisations.

**To: the Supplier**

Somerford Associates Ltd

Park House,

Church Place,

Swindon,

SN1 5ED

**Together: the ‘Parties’**

**Principle contact details**

**For the Buyer:**

Name: Mark Goodwin

Email: Mark.Goodwin@education.gov.uk

Phone: 02476 660680

**For the Supplier:**

Name: Bob Feeney

Email: Bob.Feeney@Somerfordassociates.com

Phone: 01973 698 047

## Call-Off Contract term

**Start date:** This Call-Off Contract Starts on the 20th February 2018

**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. Termination of appointment/work package from RFQ, 5 working days, but subject to agreement between Buyer and Supplier for each work package.

**Extension period:** This Call-Off Contract can be extended by the Buyer for 1 period(s) of up to 12 months by giving the Supplier 1 month’s written notice before its expiry.

Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each. Under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS) if the:

**G-Cloud lot:**

This Call-Off Contract is for the provision of Services under:

Lot 2 Cloud Software SaaS

**G-Cloud services**

**required:**

The Services to be provided by the Supplier under the above Lot are as per Service

Definition and quote below



es-8

5

8

46

n

714

d6

c5

e

p3

fd1vif.r



DFE Splunk Term

B2f-Q1

1

u2o1te7

Splunk Enterprise, Enterprise Security - 100Gb Term 1 year Licence with Enterprise

Support

Splunk Training : Splunk Enterprise Data Administration, System Administration,

Fundamentals 2 and Using Splunk Enterprise Security V4 :Maximum 6 Students

5

Days Professional Services.

**Additional services:**

Not Applicable

* Buyer is a central government department
* contract Term is intended to exceed 24 months

## Buyer contractual details

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

**Location:** The Services will be delivered to: Department of Education offices or related locations as required.

**Quality standards:** The Supplier warrants that it will carry out the services with reasonable care and skill and that all services supplied hereunder shall be of satisfactory quality and fit for the particular purpose for which they are supplied with reference to the Buyer’s requirements and in line with G-Cloud 9 offerings and in accordance with ISO 9001: 2013

The supplier is expected to work in an ‘Agile’ way, to support buyer, Digital, Data and Technology (DDaT) strategy.

Annex A – Section 1

**Technical standards: Special Clauses** Please refer to Annex A. The supplier is expected to deliver the work packages using the most appropriate project management (e.g. Agile, PRINCE2) and service management ITIL methodologies. **Service level agreement:**

**On boarding:** 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 10 the framework agreement (if any); and a forward schedule of meeting dates.

**Off boarding:** The off boarding plan for this Call-Off Contract is to be prepared by the Supplier and submitted to the Buyer within 4 weeks of the contract commencing.

This may include an exit plan of processes or costs (for example) associated with exiting the

Call-Off Contract and data standards

## Collaboration agreement: Not Applicable

**Limit on Parties’ liability:** The annual total liability of either Party for all Property defaults will not exceed £1 Million.

The annual total liability for Buyer Data defaults will not exceed £100,000 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 £100,000 or 125% 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 5 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.

* the accuracy of Charges (and proposed or actual variations to them under this

Framework Agreement)

* any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call-Off Contract only
* the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier
* any other aspect of the delivery of the Services including to review compliance with any legislation
* the accuracy and completeness of any MI delivered or required by the Framework Agreement
* any MI Reports or other records about the Supplier’s performance of the Services and to verify that these reflect the Supplier’s own internal reports and records ● the Buyer’s assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer’s assets are secure and that any asset register is up to date.

**Buyer’s responsibilities:** The Buyer is responsible for providing timely access to all sites and personnel relating to the service delivery.

**Buyer’s equipment:** Not Applicable

## Supplier’s information

**Subcontractors or**

**partners:**

Splunk Inc

## 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 30 days of the date on the invoice, by BACS for services/outputs delivered as detailed in the RFQ for each work package in accordance with Annexe B RFQ Template.

**Payment profile:** The payment profile for this Call-Off Contract is monthly in arrears.

**Invoice details:** The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.

**Who and where to send** Invoices will be sent to:

**invoices to:** Department for Education

PO Box 407

SSCL

Phoenix House, Celtic Springs Bus. Park

Newport

NP10 8FZ

Email address: APinvoices-DFE-U@sscl.gse.gov.uk **Invoice information** All invoices must include the purchase order number. **required.**

**Invoice frequency:** Invoice will be sent to the Buyer Monthly in arrears

**Call-Off Contract value:** The total value of this Call-Off Contract is £93,100.00 excluding VAT **Call-Off Contract** These will be as per the quote and G cloud rate card as below **charges:**

i641p8r518- DFE Splunk Term dopncudg6mf254.7icent B2-Q11u2o1te7

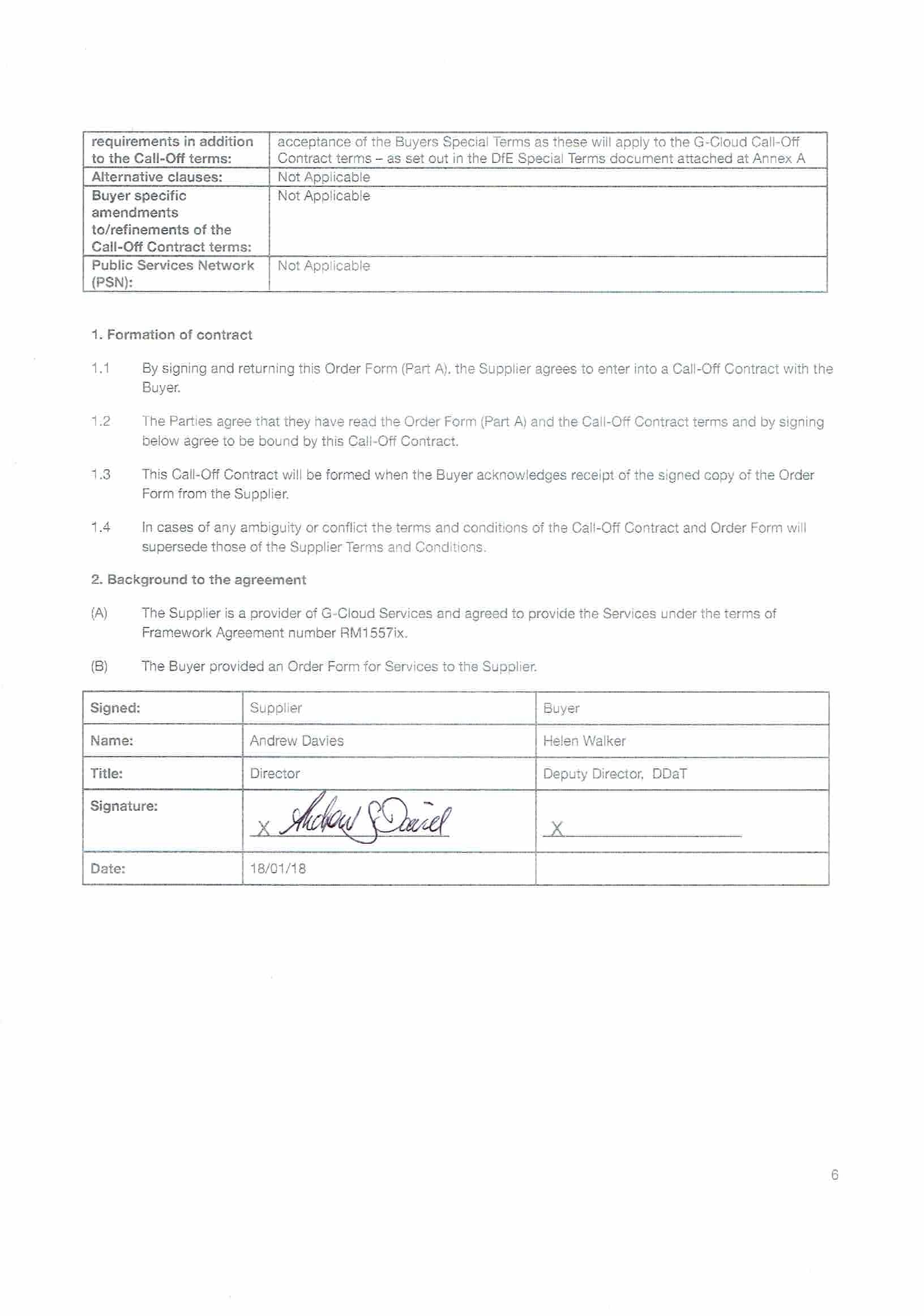
## Additional buyer terms

**Performance of the** This Call-Off Contract will include the following implementation plan, exit and off **service and deliverables:** boarding plans and milestones which will be agreed at the start up meeting as part of the on boarding process and must be provided within 4 weeks of the start up meeting.



**Guarantee:** Not Applicable **Warranties,** Not Applicable **representations:**

**Supplemental** In accordance with Call-Off Contract clauses, the Supplier must agree to unqualified



18

/01/

18

# Schedule 1 – Services

The Services will be completed in accordance to the G cloud Service Description and associated G cloud documents included in the G cloud entry below



es-8158146

e1n7146dc5p3fd1vif.r

Splunk Enterprise+Enterprise Security - 100Gb Term 1 year Licence with Enterprise Support

Splunk Training : Splunk Enterprise Data Administration, System Administration, Fundamentals 2 and Using Splunk Enterprise Security V4 :Maximum 6 Students

5 Days Professional Services

# 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 those quoted in your, Service Description, Clarification proposal and subsequent clarifications.



DFE Splunk Term

B2-Q11u2o1te7



ip6r4858-

p1on6cufg5m2.47icent

# Part B - Terms and conditions

## 1. Call-Off Contract start date and length

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

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

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

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

## 2. Incorporation of terms

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

* 4.1 (Warranties and representations)
* 4.2 to 4.7 (Liability)
* 4.11 to 4.12 (IR35)
* 5.4 to 5.5 (Force majeure)
* 5.8 (Continuing rights)
* 5.9 to 5.11 (Change of control)
* 5.12 (Fraud)
* 5.13 (Notice of fraud)
* 7.1 to 7.2 (Transparency)
* 8.3 (Order of precedence)
* 8.4 (Relationship)
* 8.7 to 8.9 (Entire agreement)
* 8.10 (Law and jurisdiction)
* 8.11 to 8.12 (Legislative change)
* 8.13 to 8.17 (Bribery and corruption)
* 8.18 to 8.27 (Freedom of Information Act)
* 8.28 to 8.29 (Promoting tax compliance)
* 8.30 to 8.31 (Official Secrets Act)
* 8.32 to 8.35 (Transfer and subcontracting)
* 8.38 to 8.41 (Complaints handling and resolution)
* 8.49 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)
* 8.57 to 8.62 (Data protection and disclosure)
* 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
  1. The Framework Agreement incorporated clauses will be referred to as ‘incorporated Framework clause XX’, where ‘XX’ is the Framework Agreement clause number.
  2. 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 CallOff 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
  1. 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.
  2. The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
  3. 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. The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
  5. 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.
  6. 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.
  7. 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.

1. **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
  1. If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
  2. 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
  1. The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
  2. 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.
  3. The Supplier will be liable for the payment of any:
* premiums, which it will pay promptly
* excess or deductibles and will not be entitled to recover this from the Buyer

## 10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all

Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Act (DPA) or under incorporated Framework Agreement clauses 8.83 to 8.91. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

## 11. Intellectual Property Rights

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

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

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

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

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

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

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

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

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

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

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services. **12. Protection of information**

12.1 The Supplier must:

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

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

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

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

## 13. Buyer data

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

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

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

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

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

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

* the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework>and the Government Security

Classification policy at [https://www.gov.uk/government/publications/government-securityclassifications](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 th](https://www.cesg.gov.uk/risk-management-collection)e 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-ofpractice](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>
  1. The Buyer will specify any security requirements for this project in the Order Form.
  2. 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.
  3. 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.
  4. 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  [T he Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the T echnology Code of Practice , which is available at h](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)[ttps://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice](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[.](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)

## 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 industryaccepted 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
  1. 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.
  2. 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>
  3. If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

## 17. Guarantee

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

* an executed Guarantee in the form at Schedule 5
* a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

## 18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving the notice to the Supplier specified in the Order Form. The Supplier’s obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

* Buyer’s right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
* Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier’s avoidable costs or Losses
  1. 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.

* 1. 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
  1. 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.
  2. 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
  1. 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.
  2. 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.

1. **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 Sent by pdf to the correct email

sending 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
  1. If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
  2. 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
  1. 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.
  2. 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
  1. 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.
  2. 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.
  3. 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.
  4. 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
  1. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
  2. 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.

# Schedule 3 - Collaboration agreement

Not Applicable

# Schedule 4 - Alternative clauses

Not Applicable

# Schedule 5 – Guarantee

Not Applicable

# Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

**Additional Services** Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.

**Admission Agreement** The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).

**Application** The response submitted by the Supplier to the Invitation to Tender (known as

the Invitation to Apply on the Digital Marketplace).

**Audit** An audit carried out under the incorporated Framework Agreement clauses

specified by the Buyer in the Order (if any).

**Background IPRs** For each Party, IPRs:

* owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes
* created by the Party independently of this Call-Off Contract, or

For the Buyer, Crown Copyright which isn’t available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.

**Buyer** The contracting authority ordering services as set out in the Order Form.

**Buyer Data** All data supplied by the Buyer to the Supplier including Personal Data and

Service Data that is owned and managed by the Buyer.

**Buyer Personal Data** The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.

**Buyer Representative** The representative appointed by the Buyer under this Call-Off Contract.

**Buyer Software** Software owned by or licensed to the Buyer (other than under this

Agreement), which is or will be used by the Supplier to provide the Services.

**Call-Off Contract** This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

**Charges** The prices (excluding any applicable VAT), payable to the Supplier by the

Buyer under this Call-Off Contract.

**Collaboration Agreement** An agreement between the Buyer and any combination of the Supplier and

contractors, to ensure collaborative working in their delivery of the Buyer’s Services and to ensure that the Buyer receives end-to-end services across its IT estate.

**Commercially Sensitive** Information, which the Buyer has been notified about by the Supplier in

**Information** 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.

**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 Protection Legislation or** The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the

**DPA** Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful

Business Practice) (Interception of Communications) Regulations 2000 (SI

2000/2699), the Electronic Communications Data Protection Directive

2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.

**Data Subject** Will have the same meaning as set out in the Data Protection Act 1998.

**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/](https://www.digitalmarketplace.service.gov.uk/))

**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** The Environmental Information Regulations 2004 together with any guidance

**Regulations or EIR** 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** The HMRC Employment Status Indicator test tool. The most up-to-date **tool or ESI tool** 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 RM1557ix 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** The Freedom of Information Act 2000 and any subordinate legislation made

**FoIA** 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.

**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** The information security management system and process developed by the **Management System** 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** Intellectual Property Rights are:

**IPR** ● 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, KnowHow, trade secrets and other rights in Confidential Information

* applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction
* all other rights having equivalent or similar effect in any country or jurisdiction

**Intermediary** For the purposes of the IR35 rules an intermediary can be:

* the supplier's own limited company
* a service or a personal service company
* a partnership

It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).

**IPR Claim** As set out in clause 11.5.

**IR35** IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect

tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.

**IR35 Assessment** Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

**Know-How** All ideas, concepts, schemes, information, knowledge, techniques,

methodology, and anything else in the nature of know-how relating to the GCloud 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.

All losses, liabilities, damages, costs, expenses (including legal fees),

**Loss** 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** As described in the Data Protection Act 1998

[(http://www.legislation.gov.uk/ukpga/1998/29/contents)](http://www.legislation.gov.uk/ukpga/1998/29/contents)

**Processing** This has the meaning given to it under the Data Protection Act 1998 as

amended but, for the purposes of this Call-Off Contract, it will include both manual and automatic processing. ‘Process’ and ‘processed’ will be interpreted accordingly.

**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.

**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 CallOff 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-ifyou-need-approval-to-spend-money-on-a-service](https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service)

**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.

**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.

**Annex A – DfE Special Clauses**

**Departmental Security Standards**

“BPSS” a level of security clearance described as pre-

“Baseline Personnel Security Standard” employment checks in the National Vetting Policy.

“CCSC” is NCSC's approach to assessing the services provided

“Certified Cyber Security Consultancy” 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-cyberconsultancy](https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy)

“CCP” is a NCSC scheme in consultation with government,

“Certified Professional” 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” the Common Criteria scheme provides assurance that a

“Common Criteria” developer’s claims about the security features of their

product are valid and have been independently tested against recognised criteria.

“CPA” is an ‘information assurance scheme’ which evaluates

“Commercial Product Assurance” commercial off the shelf (COTS) products and their

developers against published security and development

[formerly called “CESG Product Assurance”] standards. These CPA certified products can be used by

government, the wider public sector and industry. See website: [https://www.ncsc.gov.uk/scheme/commercialproduct-assurance-cpa](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa)

“Cyber Essentials” Cyber Essentials is the government backed, industry

“Cyber Essentials Plus” supported scheme to help organisations protect

themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.

“Data” shall have the meanings given to those terms by the Data

“Data Controller” Protection Act 1998

“Data Processor”

“Personal Data”

“Sensitive Personal Data”

“Data Subject”, “Process” and “Processing”

"Department’s Data" is any data or information owned or retained in order to

“Department’s Information” meet departmental business objectives and tasks,

including:

1. 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:
   1. supplied to the Contractor by or on behalf of the

Department; or

* 1. which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or

1. any Personal Data for which the Department is the Data Controller;

“DfE” means the Department for Education

“Department”

“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” means the exercise of that degree of skill, care,

“Industry Good Practice” prudence, efficiency, foresight and timeliness as would be

expected from a leading company within the relevant industry or business sector.

“Good Industry Standard” means the implementation of products and solutions, and “Industry Good Standard” 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” means the Government Security Classification Policy “GSCP” which establishes the rules for classifying HMG

information. The policy is available at:

https://www.gov.uk/government/publications/governmentsecurity-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” “Penetration Testing”

“Need-to-Know”

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.

|  |
| --- |
| 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) is the UK  government’s National Technical Authority for Information Assurance. This supersedes CESG, which was formerly the National Technical Authority. The NCSC website is [https://www.ncsc.gov.uk](https://www.ncsc.gov.uk/)  “NCSC IAP” means the NCSC (formerly CESG) Information  “NCSC Information Assurance Policy Portfolio” Assurance policy Portfolio containing HMG policy and  [Formerly called “CESG IAP”] guidance on the application of ‘security assurance’ for HMG systems.  “OFFICIAL” the term ‘OFFICIAL’ is used to describe the baseline level  “OFFICIAL-SENSITIVE” 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-sanitisationstorage-media](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)  “Security and Information Risk Advisor” the Security and Information Risk Advisor (SIRA) is a role  “CCP SIRA” defined under the NCSC Certified Professional (CCP)  Scheme. See also:  “SIRA”  [https://www.ncsc.gov.uk/articles/about-certifiedprofessional-scheme](https://www.ncsc.gov.uk/articles/about-certified-professional-scheme)  “SPF” This is the definitive HMG Security Policy which  “HMG Security Policy Framework” describes the expectations of the Cabinet Secretary and  Government’s Official Committee on Security on how |

the Need-to-Know principle is employed within HMG to

”Tailored Assurance”

[formerly called “CTAS”, or,

”CESG Tailored Assurance”] HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.

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.

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

1.2. Not Used.

1.3. The Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope

relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, 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 the ICT solution or service must be segregated from other data on the Contractor’s or sub-contractor’s own IT equipment to both protect the Departmental Data and enable it 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 and entry control mechanisms (e.g. door access) to premises and sensitive areas and separate logical access controls (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.

1.7. 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.

1.8. Any electronic transfer methods across public space or cyberspace, including third party provider networks must be protected via encryption which has been certified to a minimum of FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.

1.9. 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 1.10 and 1.11 below.

1.10. 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 a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to the Department.

1.11. 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 a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to the Department.

1.12. 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 waste paper organisation.

1.13. 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 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.

1.14. 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 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.

1.15. Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” and the appropriate level of security clearance, as required by the Department for those individuals whose access is essential for the purpose of their duties. All employees with direct or indirect access to Departmental Data must be subject to pre-employment checks equivalent to or higher than the HMG Baseline Personnel Security Standard (BPSS)

1.16. All Contractor or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.

1.17. The Contractor shall, as a minimum, have in place robust and ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures 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 be, or could lead to, a disruption, loss, emergency or crisis. When a certificate is not available it shall

be necessary to verify the ongoing effectiveness of the ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures, to the extent that the Contractor must have tested/exercised these plans within the last 12 months and produced a written report of the test/exercise, outcome and feedback, including required actions.

1.18. Any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution, or any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, 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 hold Departmental Data being handled, stored or processed in the course of providing this service shall be subject to an independent IT Health Check (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 actual storage outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management or support 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.

**Contractor’s Standards**

2.1 The Contractor shall as far as practicable satisfy the Department that it operates to an acceptable standard such as BS 5750, BS EN ISO 9000 or an equivalent.

**Annexe B RFQ Template**

**Service Provider Request for Quote**

*This form is structured in three parts: Part 1 is the Request for Quote, Part 2 is the Service Provider’s Response, Part 3 is the*

*Customers’ Acceptance, together with the guidance that should be followed to raise a Purchase Order Requisition.*

**To be completed by DDaT Contracts and Commercial Team (CCT)**

**Date Request sent to Service Provider**

**RfQ**

**Reference**

**Part 1. Request**

**for Quote.**

**To be completed by the work requester**

All requests must be completed in accordance with the DDaT commissioning process/ governance arrangements. By submitting

this form, you are confirming that all the necessary business case approvals are in place to allow the services to be sourced.

**NOTE**

:

all sections of the request for quote Part 1 must be completed in full. Any partially completed forms will be rejected

.

**Request Title / Project Name**

**Work Requester**

**Directorate /**

**Division**

**Principal Contact**

**and Role**

**Name:**

**Role:**

**Address:**

**Phone:**

**IR35 Assessment Outcome**

Note: it is the responsibility of the work package requester to complete the

[HMRC IR35 assessmen](https://www.tax.service.gov.uk/check-employment-status-for-tax/setup)

[t](https://www.tax.service.gov.uk/check-employment-status-for-tax/setup)

and attach the resulting pdf

to this Request for Quote. Failure to do so will result in this request for work quote being rejected.

**Outcome of IR35**

**assessment for this Request**

**for Quote**

The intermediaries legislation does not apply to this engagement

☐

Comments:

[

NOTE: if the outcome of the IR35 assessment is either “

*the intermediaries legislation does*

*apply to this engagement” or “unable to determine the tax status of this engagement”*

please

**stop**

and seek advice from the Contracts and Commercial Team]

**Working Arrangements**

*Please describe how you intend to work with the service provider to ensure that it is compliant with*

*IR35 guidance*

*link to central*

*(*

*guidance added when available).*

Here is a helpful reminder on the behaviours of the working arrangement:



Control

– the department is responsible for stating

what

is to be delivered. The service provider is responsible for using its own

initiative in determining how the services are to be delivered and the provision of resources to support the services [which shall

include one or more specialists].



Risk (financial)

– the financial risk of delivering the service/deliverables/outcome must lie with the service provider. Outputs and

deliverables will be linked to payments. If the work does not meet the acceptance criteria it is the responsibility of the service

provider to correct it at their own expense



Integration (part and parcel of the organisation)

-

The service provider should not be treated as one of the team or be

indispensable. They are expected to provide the services on such hours/days as required to meet any deadlines, as agreed

between the service provider and the department.



Substitution

– the department are willing to accept substitute personnel with the relevant skills and expertise from the service

provider (e.g. to cover holidays, illness etc.).



Provision of own equipment

-

The service provider must provide their own equipment where security requirements permit.

Please describe any exceptions, and the reasons for these exceptions, to this (e.g. DfE accounts, MS Azure accounts)

***This request for work is for a***

***service***

***If it looks like a people role then it probably is***

**Funding**

**Funding Team/Division**

**Cost Centre**

**Term**

**Target Commencement Date**

**Target Delivery Date**

**Work Package Objectives**

***Provide a summary of the Department's requirements, including the overall objectives and activities for the service to be provided and***

***known skills required. Please indicate if there are any requirements to visit departmental offices***

***.***

**Work Package Deliverables**

***List any specific deliverables that the Service Provider must produce. All deliverables must be defined against measurable acceptance***

***criteria.***

Ref

Deliverable Date

Deliverable Description

Acceptance Criteria (quality expected)

**Risks**

*Please identify all known risks that might affect the service provider’s ability to deliver the service requirement which meets the acceptance criteria.*

**Evaluation Criteria**

*Where this RfQ is provided to more than one company, please specify the criteria and weightings that will be used to evaluate the quotes. This*

*could include skills, experience, knowledge, substitution capacity, location, price, ability to deliver.*

**Senior Responsible Officer / Deputy Director Sign Off**

***I confirm that I have appropriate technical, project and funding approval for this proposal.***

***I accept the risk and liability in the event of an investigation by HMRC in respect of the IR35 status of this engagement.***

Name

Position

Date Finance Business Partner approval received

Date

SRO / DD Sign Off

The RfQ must now be sent to the email mailbox

ContractManagement.DDaT@education.gov.uk

.

**Part 2. Response to RfQ. To be completed by the Service Provider**

**Service Provider Response**

***Provide details on the proposal which sets out an overview of the proposed solution to the Department’s***

***Requirements.***

**Service Provider Obligations on the Department**

*Provide details of any obligations on the Department that may be necessary for the activities contained within this Work*

*Package.*

**Service Provider Costs**

*Provide the charges for this Work Package. The charges shall be constructed using the rates agreed as part of the call-off*

*contract*

*.*

**Service Provider Payment Terms and Milestones**

*Provide details on the milestones and payment terms for each milestone.*

Deliverables

Units

(

No. of days x rate

)

Price (excluding VAT)

Discounts to be applied

Total

**Deliverable**

**Milestone**

**Duration**

**Milestone**

**Date**

**Payment Terms**

**Term**

Commencement Date

Delivery Date

**Service Provider Sign Off**

*Additional comments*

Response Prepared by

Position

Signature

Date Submitted to the

Department

The RfQ must now be sent to the email mailbox

ContractManagement.DDaT@education.gov.uk

**Part 3. Evaluation, Customer Acceptance and Authority for the Work to Commence**

The department will evaluate the quotes against the work package requirement using the evaluation criteria set out in

part 1.

For the successful service provider, all relevant information from this form must now be transferred onto the appropriate

Request for Goods and Service template and passed to the nominated Requisitioner for loading onto SOPS so that a

Purchase Order can be produced. The Purchase Order is the agreement by which the customer instructs the service

provider to provide services as described in the service provider response to the work package / request for quote. The

service provider will commence the work within the agreed timeframe upon receipt of this Purchase Order. Any

Purchase Order queries should be directed to the Work Requester.

For the unsuccessful service providers, the department will notify them in a timely manner.