# GET INTO TEACHING (GIT) WEBSITE SUPPORT

## CONTRACT NO. ICT 2017-027

## G-Cloud services call-off terms

**DEPARTMENT for EDUCATION**

**- and -**

**Redweb Ltd relating to**

**the provision of G-Cloud Services**

# Contents



## Schedule 1: Call-Off Terms

**DEEMED TO BE EFFECTIVE FROM:**

| | | | |
|---|---|---|---|
| **Date** | 22 May 2017 | **Order Reference** | ICT 2017-027 |

**FROM:**

| | |
|---|---|
| Customer | The Secretary of State for Education "**Customer**" |
| Customer's Address | Sanctuary Buildings, Great Smith Street, London, SW1P3BT |

| | |
|---|---|
| Invoice Address | Invoices should be emailed in PDF format to: [redacted]<br><br>The invoices should be addressed to:<br><br>Department for Education<br>PO Box 407<br>SSCL<br>Phoenix House, Celtic Springs Bus. Park<br>Newport<br>NP10 8FZ<br><br>Each invoice will require an approved Purchase Order number to be processed for payment.<br><br>See additional guidance on submitting invoices at Section 6.2 |
| Principal Contact | Name: [redacted]<br><br>Address: Department for Education<br>[redacted]<br>Phone: [redacted] |

**TO:**

| | |
|---|---|
| Supplier | Redweb Ltd. "**Supplier**"<br><br>SERVICE ID 7945671504404619 |
| Supplier's Address | 35 Holdenhurst Road, Bournemouth, Dorset, BH8 8EJ |
| Account Manager | Name: [redacted]<br><br>Address: Redweb, 35 Holdenhurst Road, Bournemouth, Dorset, BH8 8EJ<br><br>Phone: [redacted] |

| **1. TERM** |
|---|
| **1.1 Commencement Date**<br><br>This Call-Off Agreement is deemed to effective from **22 May 2017** |

## 1.2 Expiry Date

This Call-Off Agreement shall expire on: 21 May 2018

1.2.1 This Call-Off Agreement shall expire on the date, which is 12 months after the commencement date in 1.1 unless:

- extended by the Customer by a period of up to 12 months in which case the Call-Off Agreement shall expire on the last day of the extended period; or
- the Call-Off Agreement has been terminated earlier pursuant to Clause CO-9 of the Call-Off Agreement.

1.2.1 Notice of the Customer's intention to extend the contract beyond 21 May 2018 shall be given to the Supplier in writing no later than 21 February 2018.

## 1.3 Services Requirements

1.3.1 This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilised by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

1.3.2 G-Cloud Services

| | |
|---|---|
| 1.3.2.1 Lot1 IaaS | N/A |
| 1.3.2.2 Lot 2 PaaS | N/A |
| 1.3.2.3 Lot 3 SaaS | N/A |
| 1.3.2.4 Lot 4 Specialist G-Cloud Services |  RedWeb Service Definition |
| 1.3.2.5 G-Cloud Additional Services | OPTION TO PROCURE ADDITIONAL SERVICES IN LINE WITH CUSTOMERS DETAILED REQUIREMENTS<br><br>All requests for development work, within scope of the agreement, shall be initiated by the Customer by means of a 'Request for Quote' (RFQ) which will be emailed to the Supplier's nominated representative. The work will be in the form of individual work packages, detailing the specific requirement and timescales needed. The payment profile for each work package will be linked where appropriate, to the milestones and outputs agreed between the Customer and Supplier before work initiation. |

## 2. PRINCIPAL LOCATIONS

### 2.1 Principal locations where the services are being performed:

**Redweb Premises :** Redweb, 35 Holdenhurst Road, Bournemouth, Dorset, BH8 8EJ

## 3. STANDARDS

### 3.1 Quality Standards

All delivered services will be in line with the quality standards offered or defined in the Gcloud service descriptions

### 3.2 Technical Standards

All delivered services will be in line with the technical standards offered or defined in the Gcloud service descriptions

## 4. ONBOARDING

### 4.1 On-boarding

4.1.1. All maintenance requests are logged by the customer on Jira

On-boarding is the mutual agreement and execution of the ‘variable GiT cost model’ referenced in section 8 and accompanied by completion of the milestones section 12.2 below.

4.2 All testing will conform to the agreed standards, engagement methodology and testing processes documented in this agreement and associated Redweb Gcloud Service Description documents

4.3 The Customer and Supplier shall attend a start-up meeting with representatives of the Customer (booked for 18 July.) At this meeting the agenda will include but not be limited to: discussion and agreement on activity to implement the service within the DfE including future contract management arrangements; how development work and business critical requests will be managed; project documentation and deliverables; service delivery KPIs; requirements for reporting of Management Information consistent with clause 8 of the framework agreement (if any); and a forward schedule of meeting dates.

## 5. CUSTOMER AND SUPPLIER RESPONSIBILITIES

**5.1 Customer and Supplier's Responsibilities**

1. **The contract focus is on delivery of the ongoing site hosting, support, maintenance and development of the Get Into Teaching (GIT) website.**

2. **Maintenance work requests** will be scheduled into organised sprints with one deployment per month. The supplier resource will be scheduled in advance and require a minimum of 2 weeks notice to alter bookings. All maintenance work requests will go through Jira.
3. All sprints including costs need to be signed off by the customer before the work commences. Project management will cover the sprint prioritisation at the beginning of each month and reporting at the end of the month. The supplier's PM will dial into a weekly status call regarding this work.
   The supplier and customer will agree work request process for business critical requests at the initial briefing meeting 18/7.
4. If design is required for a sprint, the supplier will be informed in the final week of the previous sprint and this may lead to substituting design for another resource, e.g. development.
5. SEO time will support the content updates and ensure any changes made to the site will not affect the SEO ranking.
6. If requirements change, the supplier will look to adjust the planned work however any time already used that month would of course be lost if the work is no longer needed

7. **For all development work**: the customer will set up a requirements workshop (either telephone or face to face) to discuss the requirements. Following this workshop, Redweb will produce a Statement of Work showing the costs and time required for the development. This needs to be signed off by the Customer prior to work commencing.

8. The supplier will dial into the monthly service and contract management calls for a maximum of 2 hours. These meetings will be attended by the Supplier, Service Manager and Contract Manager who will ensure that all relevant reporting is completed in preparation for these meetings. The Supplier may be required to attend face-to-face contract/service management meetings, and,or inter-agency meetings as requested by the Customer.

9. The supplier Service Manager will report on the KPIs and Milestones via the monthly service and contract meetings, and they will be the contract escalation point and have overall responsibility for the GiT Support Contract.

10. Support tickets will continue to be handled via Deskpro (Redweb's support system).

11. Due to strategic changes within the department there will be a requirement to review both hosting arrangements and live chat functionality during the life of the contract. There may be a strategic requirement to move hosting to the DfE enterprise version of Azure during the contract. If hosting moves to Azure and Redweb continues to support this application to some capacity, then the support costs will be reviewed. We will engage with Redweb during the contract to investigate both this and potential changes to the live chat requirements.

This is the summary of Customer and Supplier agreed high level requirements, reflected as delivery within Schedule 8 and embedded attachment below


GiT Website requirements 2017.dc

### 5.2 Customer's equipment

N/A

## 6. PAYMENT

### 6.1 Payment profile and method of payment

| | |
|---|---|
| Hosting | £3,060.50 per month |
| Live Chat | £481.50 per month |
| Azure* | £1,000 per month if the platform is hosted on Redweb's Azure instance |
| Migration to Azure | £15,225.00 |
| Support* | £3,000 per month<br>£4,800 per month if the platform is hosted on Azure and Redweb are supporting this application |
| Exit/Transition costs | £25,000 |

***hosting and support costs subject to whether website is migrated to Azure (and whether this is Redweb's Azure instance or the DfE instance), and level of support Redweb are required to provide for this application***

Maintenance Costs will be in accordance with the pricing shown on GCloud (please see attached).


RedWeb Pricing


RedWeb SFIA Rate Card

Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS

6.1.1 Monthly in arrears

**6.2 Invoice format**

The Supplier shall issue paper invoices, in arrears, on satisfactory completion of agreed work packages. The Customer shall pay the Supplier within thirty (30) calendar days of receipt of a valid invoice, submitted in accordance with this paragraph 6.2 the payment profile set out in paragraph 6.1 above and the provisions of this Call-Off Agreement.

A valid invoice is one that is:

- Delivered in timing in accordance of the contract
- Is for the correct sum
- Is correct in terms of services/goods supplied
- Has a unique invoice number
- Quotes a valid Purchase Order number
- Includes correct supplier details, date, contact details
- Invoicing will be in £ Sterling and payment will be made by BACS transfer.

Invoicing will be in £ Sterling

**All queries regarding payments or the settlement of invoices shall be directed to the team or project that placed the Purchase Order. Escalation of payment issues is to the Contract Manager:** [redacted]

## 7. DISPUTE RESOLUTION

**7.1 Level of Representative to whom disputes should be escalated to:**

For DfE: [redacted]

For Redweb: [redacted]

**7.2 Mediation Provider**

Centre for Effective Dispute Resolution.

## 8. LIABILITY

**Subject to the provisions of Clause CO 11 'Liability' of the Call–Off Agreement:**

8.1 The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party (including technical infrastructure, assets, equipment or IPR but excluding any loss or damage to the Customer Data or Customer Personal Data) under or in connection with this Call–Off Agreement shall in no event exceed £1 million.

8.2 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall in no event exceed £1 million of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period.

8.3 The annual aggregate liability under this Call–Off Agreement of either Party for all defaults shall in no event exceed the greater of £100,000 or one hundred and twenty five per cent (125%) per cent of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period.

## 9. INSURANCE

**9.1 Minimum Insurance Period**

Six (6) Years following the expiration or earlier termination of this Call-Off Agreement

**9.2 To comply with its obligations under this Call-Off Agreement and as a minimum, where requested by the Customer in writing the Supplier shall ensure that:**

- **professional indemnity insurance** is held by the Supplier and by any agent, Sub-Contractor or consultant involved in the supply of the G-Cloud Services and that such professional indemnity insurance has a minimum limit of indemnity of one million pounds sterling (£1,000,000) for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time;
- **employers' liability insurance** with a minimum limit of five million pounds sterling (£5,000,000) or such higher minimum limit as required by Law from time to time

**12.1 Implementation Plan and Milestones (including dates for completion)**

12.2 The Implementation Plan as at the Commencement Date is set out below:

| Milestone | Milestone reference | Deliverables | Duration | Milestone Date | Customer Responsibilities |
|---|---|---|---|---|---|
| Service credit regime | 1 | Agree service credit regime [as applicable] for the contract, to include quantitative and qualitative measure for performance | Service credits will be live for the contract duration | August 2017-October 2017 | Schedule milestone meeting with supplier by 19.08.17 |
| Contract Publishing Process | 2 | Agree a contract publishing process with the NCTL GiT Marketing Team | Publishing process will be live for the contract duration. | 31st August 2017 | Work with supplier to agree a publishing process which meets both the needs of NCTL /DfE and the supplier. |
| Normal and urgent work request procedure | 3 | Agree and implement a procedure for normal sprint and urgent work requests | Normal and urgent work<br><br>request procedure will be live for the<br><br>duration of the<br><br>contract | 18th July 2017 | Work with the supplier to agree a normal sprint and urgent request procedure |
| Content<br><br>Editing and Publishing Training | 4 | Deliver two training sessions on content editing and<br><br>publishing for up to 8 NCTL/DfE staff in<br><br>Manchester and London (these are across GiT and ITT teams) | Two training sessions | TBC | To identify staff to be trained, manage<br><br>invites and book rooms in Manchester and London sites. |

| | | | | | |
|---|---|---|---|---|---|
| Amend CMS permission to enable DFE staff access | 5 | To amend CMS permissions for named NCTL/DFE staff to be able to publish content to the live site. | For the duration of the contract. | TBC | |
| Add Jira access to enable DfE and other suppliers access | 6 | To amend Jira access permission for named DfE and other supplier staff | For the duration of the contract | TBC | Identify named contacts to be added. Monitor the appropriateness and volume of requests from external contacts. |
| Exit Plan | 7 | Agree an exit / transition plan | To be in place within three months of contract signature. | August to November 2017 | To support the supplier in the development of the exit /transition plan. |
| Transition of database supplier | 8 | Agree and implement a plan to support the transition to a new database/call centre/conversion supplier | If required | TBC | Work with suppliers to agree a plan |

12.2.1 If so required by the Customer, the Supplier shall produce within one (1) Month of the Commencement Date a further version of the Implementation Plan (based on the above plan) in such further detail as the Customer may reasonably require. The Supplier shall ensure that each version of the Implementation Plan is subject to Customer's written approval. The Supplier shall ensure that the Implementation Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation transition and/or transformation of the G-Cloud Services.

12.2.2 The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

12.2.3 The Supplier shall perform its obligations so as to achieve each milestone by the milestone date.

12.2.4 Changes to the milestones shall only be made in accordance with the Variation procedure as set out in Clause CO-21 and provided that the Supplier shall not attempt to postpone any of the milestones using the Variation procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a milestone by the relevant milestone date).]

**12.3 Service Levels**

**12.3.2 Key Performance Indicators**

**12.3.1 There are 8 KPIs that will be used to manage the contract and delivery within Schedule 8 and embedded attachment below**

Contract No. ICT
2017- 029 GiT Suppor

## 13. COLLABORATION AGREEMENT

In accordance with Clause CO-20 of this Call-off Agreement, the Customer does not require the Supplier to enter into a Collaboration Agreement. However the Customer requires Supplier adherence to CO-20

## 10. TERMINATION

### 10.1 Undisputed Sums Time Period

At least ninety (90) Working Days of the date of the written notice specified in Clause CO-9.4 of the Call-Off Agreement**.**

### 10.2 Termination Without Cause

At least thirty (30) Working Days in accordance with Clause CO-9.2 of the Call-Off Agreement.

## 11. AUDIT AND ACCESS

Twelve (12) Months after the expiry of the Call-Off Agreement Period or following termination of this Call-Off Agreement.

## 12. PERFORMANCE OF THE SERVICES AND DELIVERABLES

**Annex 1**

**DfE : Special Conditions for Contracts**

**1. Intellectual Property Rights and Copyright**

| | |
|---|---|
| "Intellectual Property Rights" | means patents, trademarks, service marks, design rights (whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom). |

| | |
|---|---|
| "the Act" | means the Copyright Designs and Patents Act 1988; |
| "Copyright" | means any and all copyright, design right (as defined by the Act) and all other rights of a like nature which may, during the course of this Contract, come into existence in or in relation to any Work (or any part thereof); |
| "Crown and/or Her Majesty" | both mean Queen Elizabeth II and any successor to Her Majesty; |
| "HMSO" | means Her Majesty's Stationery Office; |
| "Her Majesty's Government" | means the duly elected Government for the time being during the reign of Her Majesty and/or any department, committee, office, servant or officer of such Government; |
| "Work" | means any and all Works including but not limited to literary, dramatic, musical or artistic works, sound recordings, films, broadcasts or cable programmes, typographical arrangements and designs (as the same are defined in the Act) which are created from time to time during the course of this Contract by the Contractor or by or together with others at the Contractor's request or on its behalf and where such works directly relate to or are created in respect of the performance of this Contract or any part of it. |

1 **Intellectual Property Rights and Copyright**

1.1 The Contractor agrees that the Crown shall be legally and beneficially entitled to any and all Intellectual Property Rights and Copyright and the Contractor hereby assigns to the Crown any and all residual title which it may have in any and all such Intellectual Property Rights and/or Copyright.

1.2 The Contractor undertakes that it shall, from time to time, take all such steps and execute all such documents as the Crown or HMSO on its behalf may reasonably require to fully vest in the Crown any and all residual title, whether legal or beneficial, to the Intellectual Property Rights and/or Copyright.

**Copyright Warranties**

1.3 The Contractor now warrants to the Crown, HMSO and the Department (and to any assignees and licensees of each) that all Works will not infringe in whole or in part any copyright or like right or any other intellectual property right of any other person (wheresoever) and agrees to indemnify and hold harmless Her Majesty and/or Her Majesty's Government against any and all claims, demands, proceedings, expenses and losses, including any of a consequential nature, arising directly or indirectly out of any act of the foregoing in relation to any Work, where such act is or is alleged to be an infringement of a third party's copyright or like right or other intellectual property right (wheresoever).

1.4 The warranty and indemnity contained in Clause 1.3 above shall survive the termination of this Contract and shall exist for the life of the Copyright.

**2. Not Used**

**3. Not Used**

**4. Contractors Standards**

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.

**5. Not Used**

**6. Not Used**

**7. Not Used**

**8. Not Used**

**9. Not Used**

**10. Not Used**

**11. Data Protection Act**

| | |
|---|---|
| **"Affiliate"** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| **"Contractor Personnel"** | all employees, agents, Contractors and contractors of the Contractor and/or of any Sub-contractor; |

| | |
|---|---|
| **"Control"** | means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and **"Controls"** and **"Controlled"** shall be interpreted accordingly; |
| **"Regulatory Bodies"** | those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Department and **"Regulatory Body"** shall be construed accordingly. |
| **"Sub-contractor"** | the third party with whom the Contractor enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents; |
| **"Working Day"** | any day other than a Saturday, Sunday or public holiday in England and Wales. |

11.1 With respect to the parties' rights and obligations under this Contract, the parties agree that the Department is the Data Controller and that the Contractor is the Data Processor. For the purposes of this Clause 11, the terms "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Process" and "Processing shall have the meaning prescribed under the DPA.

11.2 The Contractor shall:

11.2.1 Process the Personal Data only in accordance with instructions from the Department (which may be specific instructions or instructions of a general nature as set out in this Contract or as otherwise notified by the Department to the Contractor during the period of the Contract);

11.2.2 Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by law or any Regulatory Body;

11.2.3 Implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

11.2.4 Take reasonable steps to ensure the reliability of any Contractor Personnel who have access to the Personal Data;

11.2.5 Obtain prior written consent from the Department in order to transfer the Personal Data to any Sub-contractors or Affiliates for the provision of the Services;

11.2.6 Ensure that all Contractor Personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Clause11;

11.2.7 Ensure that none of Contractor Personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Department;

11.2.8 Notify the Department within five Working Days if it receives:

11.2.8.1 a request from a Data Subject to have access to that person's Personal Data; or
11.2.8.2 a complaint or request relating to the Department's obligations under the Data Protection Legislation;

11.2.9 Provide the Department with full cooperation and assistance in relation to any complaint or request made, including by:

11.2.9.1 providing the Department with full details of the complaint or request;
11.2.9.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Department's instructions;
11.2.9.3 providing the Department with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Department); and
11.2.9.4 providing the Department with any information requested by the Department;

11.2.10 Permit the Department or the Department's Representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Contractor's data processing activities (and/or those of its agents, subsidiaries and Sub-contractors) and comply with all reasonable requests or directions by the Department to enable the Department to verify and/or procure that the Contractor is in full compliance with its obligations under this Contract;

11.2.11 Provide a written description of the technical and organisational methods employed by the Contractor for processing Personal Data (within the timescales required by the Department); and

11.2.12 Not Process or otherwise transfer any Personal Data outside the European Economic Area. If, after the Commencement Date, the Contractor (or any Sub-contractor) wishes to Process and/or transfer any Personal Data outside the European Economic Area, the following provisions shall apply:

11.2.12.1 the Contractor shall submit a request for change to the Department which shall be dealt with in accordance with any Change Control Procedure

11.2.12.2 the Contractor shall set out in its request for change details of the following:

(a) the Personal Data which will be Processed and/or transferred outside the European Economic Area;
(b) the country or countries in which the Personal Data will be Processed and/or to which the Personal Data will be transferred outside the European Economic Area;
(c) any Sub-contractors or other third parties who will be Processing and/or transferring Personal Data outside the European Economic Area; and
(d) how the Contractor will ensure an adequate level of protection and adequate safeguards (in accordance with the Data Protection Legislation and in particular so as to ensure the Department's compliance with the Data Protection Legislation) in respect of the Personal Data that will be Processed and/or transferred outside the European Economic Area;

11.2.12.3 in providing and evaluating the request for change, the parties shall ensure that they have regard to and comply with then-current Department, Government and Information Commissioner Office policies, procedures, guidance and codes of practice on, and any approvals processes in connection with, the Processing and/or transfers of Personal Data outside the European Economic Area and/or overseas generally; and

11.2.12.4 the Contractor shall comply with such other instructions and shall carry out such other actions as the Department may notify in writing, including:

(a) incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) in this Contract or a separate data processing agreement between the parties; and
(b) procuring that any Sub-contractor or other third party who will be Processing and/or transferring the Personal Data outside the European Economic Area enters into a direct data processing agreement with the Authority on such terms as may be required by the Department, which the Contractor acknowledges may include the incorporation of standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation)."

11.3 The Contractor shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Department to breach any of its applicable obligations under the Data Protection Legislation.

## 12. Departmental Security Standards for Business Services and ICT Contracts

| | |
|---|---|
| "BPSS"<br>"Baseline Personnel Security Standard" | a level of security clearance described as pre-employment checks in the National Vetting Policy. |
| "CESG" | is the UK government's National Technical Authority for Information Assurance. The website is http://www.cesg.gov.uk/Pages/homepage.aspx |
| "CESG IAP"<br>"CESG Information Assurance Policy Portfolio" | means the CESG Information Assurance policy Portfolio containing HMG policy and guidance on the application of 'security assurance' for HMG systems. |
| "CTAS"<br>"CESG Tailored Assurance" | is an 'information assurance scheme' which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. |
| "CPA"<br>"CESG Product Assurance" | is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. |
| "CCSC"<br>"CESG Certified Cyber Security Consultancy" | is CESG's approach to assessing the services provided by consultancies and confirming that they meet CESG'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. |

| | |
|---|---|
| “CCP”<br>“CESG Certified Professional” | is a CESG scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. |
| “CC”<br>“Common Criteria” | the Common Criteria scheme provides assurance that a developer’s claims about the security features of their product are valid and have been independently tested against recognised criteria. |
| “Cyber Essentials”<br>“Cyber Essentials Plus” | Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. |
| “Data”<br>“Data Controller”<br>“Data Processor”<br>“Personal Data”<br>“Sensitive Personal Data”<br>“Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Act 1998 |
| "Department’s Data"<br>“Department’s Information” | is any data or information owned or retained in order to meet departmental business objectives and tasks, including:<br>(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:<br>(i) supplied to the Contractor by or on behalf of the Department; or<br>(ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or<br>(b) any Personal Data for which the Department is the Data Controller; |
| “DfE”<br>“Department” | means the Department for Education |

| | |
|---|---|
| “Departmental Security Standards” | means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver. |
| “Digital Marketplace / GCloud” | the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework. |
| “FIPS 140-2” | this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled ‘Security Requirements for Cryptographic Modules’. This document is the de facto security standard used for the accreditation of cryptographic modules. |
| “Good Industry Practice”<br>“Industry Good Practice” | means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “Good Industry Standard”<br>“Industry Good Standard” | means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “GSC”<br>“GSCP” | means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications |
| “HMG” | means Her Majesty’s Government |
| “SPF”<br>“HMG Security Policy Framework” | This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. |
| “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 |

| | |
|---|---|
| IS5 | this is HMG Information Assurance Standard No. 5 - Secure Sanitisation issued by CESG |
| “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”<br>“Penetration Testing” | means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system. |
| “Need-to-Know” | the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties. |
| “OFFICIAL”<br>“OFFICIAL-SENSITIVE” | the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services.<br>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. |
| “Security and Information Risk Advisor”<br>“CCP SIRA”<br>“SIRA” | the Security and Information Risk Advisor (SIRA) is a role defined under the CESG CESG Certified Professional Scheme |

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

12.2. Where the Contractor will provide ICT products or Services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 25 September 2014, or any subsequent updated document, are mandated; that "contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme". The certification scope must be relevant to the services supplied to, or on behalf of, the Department.

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

12.4. 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).

12.5. 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 12.14.

12.6. 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.

12.7. 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.

12.8. 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.

12.9. 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 12.10 and 12.11 below.

12.10. 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.

12.11. 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.

12.12. 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.

12.13. 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.

12.14. 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 (HMG IS5) using a CESG 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.

12.15. 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 Baseline Personnel Security Standard (BPSS)

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

12.17. 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.

12.18. 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.

12.19. 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 CESG 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.

12.20. 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.

12.21. 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.

12.22. 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.

12.23. The Contractor shall deliver ICT solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current CESG Information Assurance Policy Portfolio and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:

- Existing security assurance for the services to be delivered, such as: PSN Compliance as a PSN Customer and/or as a PSN Service; CESG Tailored Assurance (CTAS); inclusion in the Common Criteria (CC) or CESG Product Assurance Schemes

(CPA); ISO 27001 / 27002 or an equivalent industry level certification. Documented evidence of any existing security assurance or certification shall be required.

- Existing HMG security accreditations that are still valid including: details of the body awarding the accreditation; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement. Documented evidence of any existing security accreditation shall be required.
- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

12.24. If no current security accreditation or assurance is held the Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation. This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a CESG Certified Cyber Security Consultancy (CCSC) or CESG Certified Professional (CCP) Security and Information Risk Advisor (SIRA)

**13. Ownership of Rights in the Deliverables and the Specially Written Software**

| | |
|---|---|
| "Intellectual Property Rights" | means patents, trade marks, service marks, design rights (whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom). |
| "Specially Written Software" | means any software written by or on behalf of the Contractor for the Department and supplied to the Department as detailed in Schedule 1. |
| " Deliverable" | means anything delivered or to be delivered under this Contract including the databases, and any reports, manuals and other documentation. |

13.1 Title to and risk in any tangible property embodying all Deliverables and Specially Written Software shall vest in the Department upon acceptance.

13.2 Notwithstanding clause 13.1, the Department shall not acquire title to the Intellectual Property Rights in any deliverables or in any Specially Written Software.

13.3 In consideration of the payment of the relevant charges the Contractor hereby grants, or shall procure that the owner of the Intellectual Property Rights in the Deliverables and/or the Specially Written Software grants, to the Department, a non-exclusive licence to use, reproduce, modify, adapt and enhance the Deliverables and the Specially Written Software. Such licence shall be perpetual and irrevocable.

13.4 The Contractor shall supply the Department with a copy of the source code of any Specially Written Software.

13.5 The Department shall be entitled to engage a third party to use, reproduce, modify and enhance the Deliverables and the Specially Written Software on behalf of the Department provided that such third party shall have entered into a confidentiality undertaking with the Department.

14. Not Used
15. Not Used
16 Not used
17. Not Used
18. Not Used
19. Not Used
20. Not Used
21 Not Used
22 Not Used
23 Not Used

24 Not Used
25 Not Used
26 Not Used
27 Not Used
28 TUPE – Not applicable
29 Not Used
30 Not Used
31 Not Used
32 Not Used

**33 Changes to the Department's Requirements**

Within each month, the Customer may request a change of delivery per sprint. This would entail a 'move' of resource from one priority to another. Any changes made must be mutually agreed between the Supplier and Customer, as per Milestone 3.

For Development costs, the Customer will require a separate Request For Quote based on their requirements. This needs to be approved by the Customer for money to be released from DfE's IT investment.

**34 Management**

The Supplier shall promptly comply with all reasonable requests or directions of the Contract Manager in respect of the Ordered G-Cloud Services.

The Supplier shall address any enquiries about procedural or contractual matters in writing to the Contract Manager. Any correspondence relating to this Call-Off Agreement shall quote the reference number set out in the Order Form

**35 Notices**

Any notices to be given under the Call-Off Agreement shall be delivered personally or sent by post or facsimile transmission to the Contract Manager (in the case of the Department) or to the address set out in this Call-Off Agreement (in the case of the Supplier). Any such notice shall be deemed to be served , if delivered personally, at the time of delivery, if sent by post, 48 hours after posting or, if sent by facsimile transmission, 12 hours after proper submission.

**36 Information Sharing Across Government**

All Central Government Departments and their Executive Agencies and Non Departmental Public Bodies are subject to control and reporting within Government. In particular, they report to the Cabinet Office and HM Treasury for all expenditure. Further, the Cabinet Office has a cross-Government role delivering overall Government policy on public procurement – including ensuring value for money and related aspects of good procurement practice.

For these purposes, the Department may disclose within Government any of the Contractor's documentation/information (including any that the Contractor considers to be confidential and/or commercially sensitive such as specific bid information) submitted by the Contractor to the Department during this Procurement. The information will not be disclosed outside Government. Contractors taking part in this competition consent to these terms as part of the competition process.

**BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES** to enter a legally binding contract with the Customer to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read the Call-Off Terms and the Order Form and by signing below agree to be bound by the terms of this Call-Off Agreement.

**For and on behalf of the Supplier:**

| | |
|---|---|
| Name and Title | [redacted] |
| Position | [redacted] |
| Signature | |
| Date | [redacted] |

**For and on behalf of the Customer:**

| | |
|---|---|
| Name and Title | [redacted] |
| Position | [redacted] |
| Signature | |
| Date | [redacted] |

## G-CLOUD SERVICES CALL-OFF TERMS

The Secretary of State for Education of Sanctuary Buildings, Great Smith Street, London

- and –

RedWeb Ltd

the provision of G-Cloud Services.

## CALL-OFF AGREEMENT TERMS AND CONDITIONS

**THIS CONTRACT** shall be deemed to be effective from 22 May 2017

**BETWEEN**

(1) The Secretary of State for Education of Sanctuary Buildings, Great Smith Street, London (the "Customer"); and

(2) Redweb Ltd, a company registered in England under company number 03420895 and whose registered office is at 35 Holdenhurst Road, Bournemouth, Dorset, BH8 8EJ (the "**Supplier**").

**IT IS AGREED AS FOLLOWS:**

### CO-1 OVERRIDING PROVISIONS

CO-1.1 The Supplier agrees to supply the G-Cloud Services and any G-Cloud Additional Services in accordance with the Call-Off Terms, including Supplier's Terms as identified in Framework Schedule 1 (G-Cloud Services) and incorporated into this Call-Off Agreement.

CO-1.2 In the event of and only to the extent of any conflict or ambiguity between the Clauses of this Call-Off Agreement, the provisions of the Schedules, any document referred to in the Clauses of this Call-Off Agreement (including Supplier's Terms) and the Framework Agreement, the conflict shall be resolved in accordance with the following order of precedence:

CO-1.2.1 the Framework Agreement (excluding Framework Schedule 2);

CO-1.2.2 the Clauses of this Call-Off Agreement (excluding Supplier Terms);

CO-1.2.3 the completed Order Form;

CO-1.2.4 the Collaboration Agreement (Framework Schedule 7);

CO-1.2.5 the Supplier's Terms as set out in the Framework Schedule 1 (G-Cloud Services); and

CO-1.2.6 any other document referred to in the Clauses of this Call-Off Agreement.

CO-1.3 The Supplier acknowledges and accepts that the order of prevailing provisions in this Call-Off Agreement is as set out in Clause CO-1.2 above.

## CO-2 PREVENTION OF BRIBERY AND CORRUPTION

CO-2.1 If the Supplier breaches

CO-2.1.1 Clauses FW-22.1 or FW-22.2 of the Framework Agreement; or,

CO-2.1.2 the Bribery Act 2010 in relation to the Framework Agreement

CO-2.1.3 the Customer may terminate this Call-Off Agreement.

CO-2.2 The Parties agree that the Management Charge payable in accordance with Clause FW-9 does not constitute an offence under section 1 of the Bribery Act 2010.

## CO-3 PROTECTION OF INFORMATION

CO-3.1 The provisions of this Clause CO-3, shall apply during the Call-Off Agreement Period and for such time as the Supplier holds the Customer Personal Data.

CO-3.2 The Supplier shall and shall procure that Supplier's Staff comply with any notification requirements under the DPA and both Parties undertake to duly observe all their obligations under the DPA which arise in connection with the Call-Off Agreement.

CO-3.3 To the extent that the Supplier is Processing the Order Personal Data the Supplier shall:

CO-3.3.1 ensure that it has in place appropriate technical and organisational measures to ensure the security of the Order Personal Data (and to guard against unauthorised or unlawful Processing of the Order Personal Data and against accidental loss or destruction of, or damage to, the Order Personal Data; and

CO-3.3.2 provide the Customer with such information as the Customer may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA;

CO-3.3.3 promptly notify the Customer of any breach of the security measures to be put in place pursuant to this Clause; and

CO-3.3.4 ensure that it does not knowingly or negligently do or omit to do anything which places the Customer in breach of its obligations under the DPA.

CO-3.4 To the extent that the Supplier Processes Service Personal Data the Supplier shall:

CO-3.4.1 Process Service Personal Data only in accordance with written instructions from the Customer as set out in this Call-Off Agreement;

CO-3.4.2 Process the Service Personal Data only to the extent, and in such manner, as is necessary for the provision of the G-Cloud Services or as is required by Law or any Regulatory Body;

CO-3.4.3 implement appropriate technical and organisational measures to protect Service Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to Service Personal Data and having regard to the nature of the Service Personal Data which is to be protected;

CO-3.4.4 take reasonable steps to ensure the reliability of any Supplier Staff who have access to Service Personal Data;

CO-3.4.5 ensure that all Supplier Staff required to access Service Personal Data are informed of the confidential nature of the Service Personal Data and comply with the obligations set out in this Clause;

CO-3.4.6 ensure that none of the Supplier Staff publish, disclose or divulge Customer's Personal Data to any third party unless necessary for the provision of the G-Cloud Services under the Call-Off Agreement and/or directed in writing to do so by the Customer;

CO-3.4.7 notify the Customer within five (5) Working Days if it receives:

CO-3.4.7.1 a request from a Data Subject to have access to Service Personal Data relating to that person; or

CO-3.4.7.2 a complaint or request relating to the Customer's obligations under the Data Protection Legislation;

CO-3.4.8 provide the Customer with full cooperation and assistance in relation to any complaint or request made relating to Service Personal Data, including by:

CO-3.4.8.1 providing the Customer with full details of the complaint or request;

CO-3.4.8.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Customer's instructions;

CO-3.4.8.3 providing the Customer with any Service Personal Data it holds in relation to a Data Subject (within the timescales required by the Customer); and

CO-3.4.8.4 providing the Customer with any information requested by the Data Subject.

CO-3.5 The Supplier shall:

CO-3.5.1 permit the Customer or the Customer's Representative (subject to the reasonable and appropriate confidentiality undertakings), to inspect and audit the Supplier's data Processing activities (and/or those of its agents, subsidiaries and Sub-Contractors) or provide to the Customer an independent third party inspection and audit certificate in lieu of the same (unless otherwise agreed between the Parties, the option of providing a certificate in lieu shall not be available at IL3 and above) and shall comply with all reasonable requests or directions by the Customer to enable the Customer to verify and/or procure that the Supplier is in full compliance with its obligations under this Call-Off Agreement; and/or

CO-3.5.2 subject to Clause CO-3.6 agree to an appointment of an independent auditor selected by the Supplier to undertake the activities in Clause CO-3.5.1 provided such selection is acceptable to the Customer or Customer Representative (subject to such independent auditor complying with the reasonable and appropriate confidentiality undertakings).

CO-3.6 The Supplier Shall:

CO-3.6.1 obtain prior written consent from the Customer in order to transfer Customer Personal Data to any other person (including for the avoidance of doubt any Sub-Contractors) for the provision of the G-Cloud Services;

CO-3.6.2 not cause or permit to be Processed, stored, accessed or otherwise transferred outside the EEA any Customer Personal Data supplied to it by the Customer without the prior written consent of the Customer. Where the Customer consents to such Processing, storing, accessing or transfer outside the European Economic Area the Supplier shall:

CO-3.6.3 comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is so processed, stored, accessed or transferred;

CO-3.6.4 comply with any reasonable instructions notified to it by the Customer and either:

CO-3.6.5 incorporate standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) or warrant that that the obligations set out in the Supplier Terms provide Adequate protection for Personal Data.

CO-3.7 The Supplier shall not perform its obligations under this Call-Off Agreement in such a way as to cause the Customer to breach any of its applicable obligations under the Data Protection Legislation.

CO-3.8 The Supplier acknowledges that, in the event that it breaches (or attempts or threatens to breach) its obligations relating to Customer Personal Data that the Customer may be irreparably harmed (including harm to its reputation). In such circumstances, the Customer may proceed directly to court and seek injunctive or other equitable relief to remedy or prevent any further breach (or attempted or threatened breach).

## CO-4 CONFIDENTIALITY

CO-4.1 Except to the extent set out in this Clause or where disclosure is expressly permitted elsewhere in this Call-Off Agreement, each Party shall:

CO-4.1.1 treat the other Party's Confidential Information as confidential and safeguard it accordingly; and

CO-4.1.2 not disclose any Confidential Information belonging to the other Party to any other person without the prior written consent of the other Party, except to such persons and to such extent as may be necessary for the performance of this Call-Off Agreement.

CO-4.2 The Supplier may only disclose the Customer's Confidential Information to the Supplier Staff who are directly involved in the provision of the G-Cloud Services and who need to know the information, and shall ensure that such Supplier Staff are aware of and shall comply with these obligations as to confidentiality.

CO-4.3 The Supplier shall not, and shall procure that the Supplier Staff do not, use any of the Customer's Confidential Information received otherwise than for the purposes of this Call-Off Agreement.

CO-4.4 The provisions of Clauses CO-4.1 shall not apply to the extent that:

CO-4.4.1 such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under Clause CO-7 (Transparency) and the FOIA, the Ministry of Justice Code or the Environmental Information Regulations pursuant to Clause CO-6 (Freedom of Information);

CO-4.4.2 such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

CO-4.4.3 such information was obtained from a third party without obligation of confidentiality;

CO-4.4.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Call-Off Agreement; or

CO-4.4.5 it is independently developed without access to the other Party's Confidential Information.

CO-4.5 Nothing in this Call-Off Agreement shall prevent the Customer from disclosing the Supplier's Confidential Information (including the Management Information obtained under Clause FW-8 (Provision of Management Information) of the Framework Agreement):

CO-4.5.1 for the purpose of the examination and certification of the Customer's accounts;

CO-4.5.2 for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Customer has used its resources;

CO-4.5.3 to any Crown body or any Other Contracting Body. All Crown bodies or Contracting Bodies receiving such Supplier's Confidential Information shall be entitled to further disclose the Supplier's Confidential Information to other Crown bodies or Other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown body or any Contracting Body; or

CO-4.5.4 to any consultant, contractor or other person engaged by the Customer (on the basis that the information shall be held by such consultant, contractor or other person in confidence and is not to be disclosed to any third party) or any person conducting a Cabinet Office or ERG Gateway review or any additional assurance programme.

CO-4.6 In the event that the Supplier fails to comply with Clauses CO-4.1 to Clause CO-4.4, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by notice in writing.

CO-4.7 In order to ensure that no unauthorised person gains access to any Confidential Information or any data obtained in performance of this Call-Off Agreement, the Supplier undertakes to maintain adequate security arrangements that meet the requirements of Good Industry Practice.

CO-4.8 The Supplier will immediately notify the Customer of any breach of security in relation to Customer Confidential Information obtained in the performance of this Call-Off Agreement and will keep a record of such breaches. The Supplier will use its best endeavours to recover such Customer Confidential Information however it may be recorded. This obligation is in addition to the Supplier's obligations under Clauses CO-4.1 to Clause CO-4.4. The Supplier will co-operate with the Customer in any investigation that the Customer considers necessary to undertake as a result of any breach of security in relation to Customer Confidential Information.

CO-4.9 Subject always to Clause CO-11.4 the Supplier shall, at all times during and after the Call-Off Agreement Period, indemnify the Customer and keep the Customer fully indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against the Customer arising from any breach of the Supplier's obligations under the DPA or this Clause CO-4 (Confidentiality) except and to the extent that such liabilities have resulted directly from the Customer's instructions.

## CO-5 CUSTOMER DATA

CO-5.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Customer Data.

CO-5.2 The Supplier shall not store, copy, disclose, or use the Customer Data except as necessary for the performance by the Supplier of its obligations under this Call-Off Agreement or as otherwise expressly approved by the Customer.

CO-5.3 The Supplier shall ensure that any system on which the Supplier holds any Customer Data, including back-up data, is a secure system that complies with the Supplier security policy.

## STATUTORY OBLIGATIONS AND REGULATIONS

## CO-6 FREEDOM OF INFORMATION

CO-6.1 The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and co-operate with the Customer to enable the Customer to comply with its Information disclosure obligations.

CO-6.2 The Supplier shall:

CO-6.2.1 transfer to the Customer all Requests for Information that it receives as soon as practicable and in any event within two (2) Working Days of receiving a Request for Information;

CO-6.2.2 provide the Customer with a copy of all Information, relating to a Request for Information, in its possession or control, in the form that the Customer requires within five (5) Working Days (or such other period as the Customer may specify) of the Customer's request; and

CO-6.2.3 provide all necessary assistance as reasonably requested by the Customer to enable the Customer to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

CO-6.3 The Customer shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Call-Off Agreement or any other agreement whether the Commercially Sensitive Information and/or any other

Information (including Supplier's Confidential Information) is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.

CO-6.4 In no event shall the Supplier respond directly to a Request for Information unless authorised in writing to do so by the Customer.

CO-6.5 The Supplier acknowledges that the Customer may, acting in accordance with the Ministry of Justice Code, be obliged under the FOIA, or the Environmental Information Regulations to disclose Information concerning the Supplier or the G-Cloud Services:

CO-6.5.1 in certain circumstances without consulting the Supplier; or

CO-6.5.2 following consultation with the Supplier and having taken its views into account;

provided always that where Clause CO-6.5.1 applies the Customer shall, in accordance with any recommendations of the Ministry of Justice Code, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

CO-6.5.3 The Supplier acknowledges that the description of information as Commercially Sensitive Information in Framework Schedule 6 (Interpretations and Definitions) is of an indicative nature only and that the Customer may be obliged to disclose it in accordance with this Clause CO-6.

## CO-7 TRANSPARENCY

CO-7.1 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Call-Off Agreement is not Confidential Information. The Customer shall be responsible for determining in its absolute discretion whether any of the content of this Call-Off Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

CO-7.2 Notwithstanding any other term of this Call-Off Agreement, the Supplier hereby gives its consent for the Customer to publish this Call-Off Agreement in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted), including from time to time agreed changes to this Call-Off Agreement, to the general public.

CO-7.3 The Customer may consult with the Supplier to inform its decision regarding any redactions but the Customer shall have the final decision in its absolute discretion.

CO-7.4 The Supplier shall assist and cooperate with the Customer to enable the Customer to publish this Call-Off Agreement.

## CO-8 OFFICIAL SECRETS ACTS

CO-8.1 The Supplier shall comply with and shall ensure that the Supplier Staff comply with, the provisions of:

CO-8.1.1 the Official Secrets Act 1911 to 1989; and

CO-8.1.2 Section 182 of the Finance Act 1989.

CO-8.2 In the event that the Supplier or the Supplier Staff fails to comply with this Clause, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by giving notice in writing to the Supplier.

## CO-9 TERM AND TERMINATION

CO-9.1 This Call-Off Agreement shall take effect on the Effective Date and shall expire on:

CO-9.1.1 the date specified in paragraph 1.2 of the Order Form; or

CO-9.1.2 twenty four (24) Months after the Effective Date, whichever is the earlier, unless terminated earlier pursuant to this Clause CO-9.

CO-9.2 Termination without Cause

CO-9.2.1 The Customer shall have the right to terminate this Call-Off Agreement at any time by giving the length of written notice to the Supplier as set out in paragraph 10.2 of the Order Form.

CO-9.3 Termination on Change of Control

CO-9.3.1 The Supplier shall notify the Customer immediately if the Supplier undergoes a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 ("**Change of Control**") and provided this does not contravene any Law shall notify the Customer immediately in writing of any circumstances suggesting that a Change of Control is planned or in contemplation. The Customer may terminate the Call-Off Agreement by notice in writing with immediate effect within six (6) Months of:

CO-9.3.1.1 being notified in writing that a Change of Control has occurred or is planned or in contemplation; or

CO-9.2.1.2 where no notification has been made, the date that the Customer becomes aware of the Change of Control,

but shall not be permitted to terminate where a written approval was granted prior to the Change of Control.

CO-9.3.2 For the purposes of Clause CO-9.3.1, any transfer of shares or of any interest in shares by its affiliate company where such transfer forms part of a bona fide reorganisation or restructuring shall be disregarded.

CO-9.4 Termination by Supplier

CO-9.4.1 If the Customer fails to pay the Supplier undisputed sums of money when due, the Supplier shall notify the Customer in writing of such failure to pay and allow the Customer five (5) calendar days to settle undisputed invoice. If the Customer fails to pay such undisputed sums within allotted additional 5 calendar days, the Supplier may terminate this Call-Off Agreement subject to giving the length of notice as specified in paragraph 10.1 of the Order Form.

CO-9.5 Termination on Insolvency

CO-9.5.1 The Customer may terminate this Call-Off Agreement with immediate effect by notice in writing where the Supplier:

CO-9.5.1.1 being an individual, or where the Supplier is a firm, any partner or partners in that firm who together are able to exercise direct or indirect control, as defined by Section 416 of the Income and Corporation Taxes Act 1988, and:

CO-9.5.1.2 shall at any time become bankrupt or shall have a receiving order or administration order made against him or shall make any composition or arrangement with or for the benefit of his creditors, or shall make any conveyance or assignment for the benefit of his creditors, or shall purport so to do, or appears unable to pay or to have no reasonable prospect of being able to pay a debt within the meaning of Section 268 of the Insolvency Act 1986, or any similar event occurs under the law of any other jurisdiction; or

CO-9.5.1.3 a creditor or encumbrancer attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Supplier's assets and such attachment or process is not discharged within fourteen (14) calendar days; or

CO-9.5.1.4 he dies or is adjudged incapable of managing his affairs within the meaning of Part VII of the Mental Health Act 1983; or

CO-9.5.1.5 the Supplier suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business.

CO-9.5.2 being a company, passes a resolution, or the Court makes an order that the Supplier or its Parent Company be wound up otherwise than for the purpose of a bona fide reconstruction or amalgamation, or a receiver, manager or administrator on behalf of a creditor is appointed in respect

of the business or any part thereof of the Supplier or its Parent Company (or an application for the appointment of an administrator is made or notice to appoint an administrator is given in relation to the Supplier or its Parent Company), or circumstances arise which entitle the Court or a creditor to appoint a receiver, manager or administrator or which entitle the Court otherwise than for the purpose of a bona fide reconstruction or amalgamation to make a winding-up order, or the Supplier or its Parent Company is unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986 (except where the claim is made under Section 123(1)(a) and is for an amount of less than ten thousand pounds (£10,000)) or any similar event occurs under the law of any other jurisdiction.

CO-9.6 Termination on Material Breach

CO-9.6.1 The Customer may terminate this Call-Off Agreement with immediate effect by giving written notice to the Supplier if the Supplier commits a Material Breach of any obligation under this Call-Off Agreement and if:

CO-9.6.1.1 the Supplier has not remedied the Material Breach within thirty (30) Working Days (or such other longer period as may be specified by the Customer) of written notice to the Supplier specifying the Material Breach and requiring its remedy; or

CO-9.6.1.2 the Material Breach is not, in the opinion of the Customer capable of remedy.

CO-9.7 Termination for repeated Default

CO-9.7.1 If there are two or more Defaults (of a similar nature) that will be deemed a breach for Material Breach. Where the Customer considers that the Supplier has committed a repeated Default in relation to this Call-Off Agreement or any part thereof (including any part of the G-Cloud Services) and believes that the Default is remediable, then the Customer shall be entitled to serve a notice on the Supplier:

CO-9.7.1.1 specifying that it is a formal warning notice;

CO-9.7.1.2 giving reasonable details of the breach; and

CO-9.7.1.3 stating that such breach is a breach which, if it recurs or continues, may result in a termination of this Call-Off Agreement or that part of the G-Cloud Services affected by such breach.

CO-9.7.2 If, thirty (30) Working Days after service of a formal warning notice as described in Clause CO-9.7, the Supplier has failed to demonstrate to the satisfaction of the Customer that the breach specified has not

continued or recurred and that the Supplier has put in place measures to ensure that such breach does not recur, then the Customer may deem such failure to be a Material Breach not capable of remedy for the purposes of Clause CO-9.6.1.2.

CO-9.8 The termination (howsoever arising) or expiry of this Call-Off Agreement pursuant to this Clause 9 shall be without prejudice to any rights of either the Customer or the Supplier that shall have accrued before the date of such termination or expiry.

CO-9.9 Save as aforesaid, the Supplier shall not be entitled to any payment from the Customer after the termination (howsoever arising) or expiry of this Call-Off Agreement.

## CO-10 CONSEQUENCES OF SUSPENSION, TERMINATION AND EXPIRY

CO-10.1 Where a Customer has the right to terminate a Call-Off Agreement, it may elect to suspend this Call-Off Agreement and its performance.

CO-10.2 Notwithstanding the service of a notice to terminate this Call-Off Agreement or any part thereof, the Supplier shall continue to provide the Ordered G-Cloud Services until the date of expiry or termination (howsoever arising) of this Call-Off Agreement (or any part thereof) or such other date as required under this Clause CO-10.

CO-10.3 Within ten (10) Working Days of the earlier of the date of expiry or termination (howsoever arising) of this Call-Off Agreement, the Supplier shall return (or make available) to the Customer:

CO-10.3.1 any data (including (if any) Customer Data), Customer Personal Data and Customer Confidential Information in the Supplier's possession, power or control, either in its then current format or in a format nominated by the Customer (in which event the Customer will reimburse the Supplier's pre-agreed and reasonable data conversion expenses), together with all training manuals, access keys and other related documentation, and any other information and all copies thereof owned by the Customer, save that it may keep one copy of any such data or information for a period of up to twelve (12) Months to comply with its obligations under the Framework Schedule FW-5, or such period as is necessary for such compliance (after which time the data must be deleted); and

CO-10.3.2 any sums prepaid in respect of Ordered G-Cloud Services not provided by the date of expiry or termination (howsoever arising) of this Call-Off Agreement.

CO-10.4 The Customer and the Supplier shall comply with the exit and service transfer arrangements as per the Supplier's terms and conditions identified in Framework Schedule 1 (G-Cloud Services).

CO-10.5 Subject to Clause CO-11 (Liability), where the Customer terminates this Call-Off Agreement under Clause CO-9.2 (Termination without Cause), the Customer shall indemnify the Supplier against any reasonable and proven commitments, liabilities or expenditure which would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Call-Off Agreement, provided that the Supplier takes all reasonable steps to mitigate such loss. Where the Supplier holds insurance, the Supplier shall reduce its unavoidable costs by any insurance sums available. The Supplier shall submit a fully itemised and costed list of such loss, with supporting evidence, of losses reasonably and actually incurred by the Supplier as a result of termination under Clause CO-9.2 (Termination without Cause).

**CO-11LIABILITY**

CO-11.1 Nothing in this Clause CO-11 shall affect a Party's general duty to mitigate its loss.

CO-11.2 Nothing in this Call-Off Agreement shall be construed to limit or exclude either Party's liability for:

CO-11.2.1 death or personal injury caused by its negligence or that of its staff;

CO-11.2.2 bribery, Fraud or fraudulent misrepresentation by it or that of its staff;

CO-11.2.3 any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982; or

CO-11.2.4.any other matter which, by Law, may not be excluded or limited.

CO-11.3 Nothing in this Call-Off Agreement shall impose any liability on the Customer in respect of any liability incurred by the Supplier to any other person, but this shall not be taken to exclude or limit any liability of the Customer to the Supplier that may arise by virtue of either a breach of the Call-Off Agreement or by negligence on the part of the Customer, or the Customer's employees, servants or agents.

CO-11.4 Subject always to Clause CO-11.2, the aggregate liability of either Party under or in connection with each Year of this Call-Off Agreement (whether expressed as an indemnity or otherwise):

CO-11.4.1 for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to the Customer Personal Data or Customer Data ) of the other Party, shall be subject to the financial limits set out in paragraph 8.1 of the Order Form;

CO-11.4.2 and in respect of all other defaults, claims, losses or damages, whether arising from breach of contract, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory

duty or otherwise shall not exceed a sum equivalent to the financial limit set out in paragraph 8.3 of the Order Form .

CO-11.5 Subject always to Clause CO-11.4 the Customer shall have the right to recover as a direct loss:

CO-11.5.1 any additional operational and/or administrative expenses arising from the Supplier's Default;

CO-11.5.2 any wasted expenditure or charges rendered unnecessary and/or incurred by the Customer arising from the Supplier's Default; and

CO-11.5.3 any losses, costs, damages, expenses or other liabilities suffered or incurred by the Customer which arise out of or in connection with the loss of, corruption or damage to or failure to deliver Customer Data by the Supplier.

CO-11.6 The Supplier shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Call-Off Agreement.

CO-11.7 Subject to Clauses CO-11.2 and Clause CO-11.5, in no event shall either Party be liable to the other for any:

CO-11.7.1 loss of profits;

CO-11.7.2 loss of business;

CO-11.7.3 loss of revenue;

CO-11.7.4 loss of or damage to goodwill;

CO-11.7.5 loss of savings (whether anticipated or otherwise); and/or

CO-11.7.6 any indirect, special or consequential loss or damage.

CO-11.8 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall be subject to the financial limits set out in paragraph 8.2 of the Order Form.

## CO-12 INSURANCE

CO-12.1 The Supplier shall effect and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under this Call-Off Agreement, including death or personal injury, loss of or damage to property or any other loss (including the

insurance policies specified in the relevant paragraph of the Order Form). Such policies shall include cover in respect of any financial loss arising from any advice given or omitted to be given by the Supplier. Such insurance shall be maintained for the Call-Off Agreement Period and for the minimum insurance period as set out in paragraph 9 of the Order Form.

CO-12.2 The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under this Call-Off Agreement.

## CO-13 PAYMENT, VAT AND CALL-OFF AGREEMENT CHARGES

CO-13.1 In consideration of the Supplier's performance of its obligations under this Call-Off Agreement, the Customer shall pay the Charges in accordance with the Clause CO-13.2 to CO-13.8.

CO-13.2 The Customer shall pay all sums properly due and payable to the Supplier in cleared funds within the time period specified in paragraph 6 of the Order Form.

CO-13.3 The Supplier shall ensure that each invoice contains all appropriate references and a detailed breakdown of the G-Cloud Services supplied and that it is supported by any other documentation reasonably required by the Customer to substantiate the invoice.

CO-13.4 Where the Supplier enters into a Sub-Contract it shall ensure that a provision is included in such Sub-Contract which requires payment to be made of all sums due by the Supplier to the Sub-Contractor within a specified period not exceeding thirty (30) calendar days from the receipt of a validly issued invoice, in accordance with the terms of the Sub-Contract.

CO-13.5 The Supplier shall add VAT to the Charges at the prevailing rate as applicable.

CO-13.6 The Supplier shall fully indemnify the Customer on demand and keep the Customer fully indemnified on a continuing basis against any liability, including without limitation against any interest, penalties or costs, which are suffered or incurred by or levied, demanded or assessed on the Customer at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Call-Off Agreement. Any amounts due under this Clause CO-13.6 shall be paid by the Supplier to the Customer not less than five (5) Working Days before the date upon which the tax or other liability is payable by the Customer.

CO-13.7 The Supplier shall not suspend the supply of the G-Cloud Services unless the Supplier is entitled to terminate this Call-Off Agreement under Clause CO-9.4 for Customer’s failure to pay undisputed sums of money. Interest shall be payable by the Customer on the late payment of any undisputed sums of money properly invoiced in accordance with the Late Payment of Commercial Debts (Interest) Act 1998 (as amended from time to time).

CO-13.8 In the event of a disputed invoice, the Customer shall make payment in respect of any undisputed amount in accordance with the provisions of Clause CO-13 of this Call-Off Agreement and return the invoice to the Supplier within ten (10) Working Days of receipt with a covering statement proposing amendments to the invoice and/or the reason for any non-payment. The Supplier shall respond within ten (10) Working Days of receipt of the returned invoice stating whether or not the Supplier accepts the Customer's proposed amendments. If it does then the Supplier shall supply with the response a replacement valid invoice.

CO-13.9 The Supplier shall accept the Government Procurement Card as a means of payment for the G-Cloud Services where such card is agreed with the Customer to be a suitable means of payment. The Supplier shall be solely liable to pay any merchant fee levied for using the Government Procurement Card and shall not be entitled to recover this charge from the Customer.

## CO-14 GUARANTEE

CO-14.1 Where the Customer has specified in the Order Form that this Call-Off Agreement shall be conditional upon receipt of a Guarantee from the guarantor, the Supplier shall deliver to the Customer an executed Guarantee from the guarantor, on or prior to the Commencement Date; and deliver to the Customer a certified copy of the passed resolution and/or board minutes of the guarantor approving the execution of the Guarantee.

## CO-15 FORCE MAJEURE

CO-15.1 Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Agreement to the extent that such delay or failure is a result of Force Majeure.

CO-15.2 Notwithstanding Clause CO-15.1, each Party shall use all reasonable endeavours to continue to perform its obligations under the Call-Off Agreement for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under this Call-Off Agreement for a period in excess of one hundred and twenty (120) calendar days, either Party may terminate this Call-Off Agreement with immediate effect by notice in writing to the other Party.

## CO-16 TRANSFER AND SUB-CONTRACTING

CO-16.1 The Supplier shall not assign, novate, sub-contract or in any other way dispose of this Call-Off Agreement or any part of it without the Customer's prior written approval which shall not be unreasonably withheld or delayed. Sub-Contracting any part of this Call-Off Agreement shall not relieve the Supplier of any obligation or duty attributable to the Supplier under this Call-Off Agreement.

CO-16.2 The Supplier shall be responsible for the acts and omissions of its Sub-Contractors as though they are its own.

CO-16.3 The Customer may assign, novate or otherwise dispose of its rights and obligations under the Call-Off Agreement or any part thereof to:

CO-16.3.1 any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Customer; or

CO-16.3.2 any private sector body which substantially performs the functions of the Customer

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier's obligations under the Call-Off Agreement.

## CO-17 THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

CO-17.1 A person who is not party to this Call-Off Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Call-Off Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

## CO-18 LAW & JURISDICTION

CO-18.1 This Call-Off Agreement and/or any non-contractual obligations or matters arising out of or in connection with it, shall be governed by and construed in accordance with the Laws of England and Wales and without prejudice to the dispute resolution procedures set out in Clause FW-14 or CO-22 (Dispute Resolution) each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

## CO-19 ADDITIONAL G-CLOUD SERVICES

CO-19.1 The Customer may require the Supplier to provide the Additional G-Cloud Services. The Supplier acknowledges that the Customer is not obliged to take any Additional G-Cloud Services from the Supplier and that there is nothing preventing the Customer from receiving services that are the same as or similar to the Additional G-Cloud Services from any third party.

CO-19.2 The Supplier shall provide Additional G-Cloud Services in accordance with any relevant Implementation Plan(s) and the Supplier shall monitor the performance of such Additional G-Cloud Services against the Implementation Plan(s).

## CO-20 [COLLABORATION AGREEMENT

CO-20.1 The Customer has specified in paragraph 13 of the Order Form that the Customer does not require the Supplier to enter into a full Collaboration Agreement, however, the Customer expects the supplier to meet the obligations in CO-20.2.

CO-20.2 In addition to its obligations under any Collaboration Agreement, the Supplier shall:

CO-20.2.1 work pro-actively with each of the Customer's contractors in a spirit of trust and mutual confidence;

CO-20.2.2 in addition to its obligations under the Collaboration Agreement the Supplier shall cooperate with the Customer's contractors of other services to enable the efficient operation of the ICT services; and

CO-20.2.3 assist in sharing information with the Customer's contractors for the purposes of facilitating adequate provision of the G-Cloud Services and/or Additional G-Cloud Services.

## CO-21 VARIATION PROCEDURE

CO-21.1 The Customer may request in writing a variation to this Call-Off Agreement provided that such variation does not amount to a material change of the Framework Agreement and/or this Call-Off Agreement and is within the meaning of the Regulations and the Law. Such a change once implemented is hereinafter called a **"Variation**".

CO-21.2 The Supplier shall notify the Customer immediately in writing of any changes proposed or in contemplation in relation to G-Cloud Services or their delivery by submitting Variation request. For the avoidance of doubt such changes would include any changes within the Supplier's supply chain.

CO-21.3 In the event that:

(a) Either Party is unable to agree (agreement shall not be unreasonably withheld or delayed) to or provide the Variation;

(b) the Customer may:

(i) agree to continue to perform its obligations under this Call-Off Agreement without the Variation; or

(ii) terminate this Call-Off Agreement by giving thirty (30) written days notice to the Supplier.

## CO-22 DISPUTE RESOLUTION

CO-22.1 The Customer and the Supplier shall attempt in good faith to negotiate a settlement of any dispute between them arising out of or in connection with this Call-Off Agreement within twenty (20) Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the Customer Representative and the Supplier Representative.

CO-22.2 If the dispute cannot be resolved by the Parties pursuant to this Clause, the Parties shall refer it to mediation unless the Customer considers that the dispute is not suitable for resolution by mediation.

CO-22.3 If the dispute cannot be resolved by mediation the Parties may refer it to arbitration.

CO-22.4 The obligations of the Parties under this Call-Off Agreement shall not be suspended, cease or be delayed by the reference of a dispute to mediation or arbitration pursuant to this Clause and the Supplier and Supplier's Staff shall continue to comply fully with the requirements of this Call-Off Agreement at all times.

**Schedule 4: Not Used**

**Schedule 5: Not Used**

**Schedule 6: Not Used**

**Schedule 7: Not Used**

**Schedule 8: Not Used**

**Schedule 9: Not Used**

**Schedule 10: Not Used**