



# Crown Commercial Service

## G-Cloud 10 Call-Off Contract

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

<b>Part A - Order Form</b>	<b>2</b>
<b>Schedule 1 - Services</b>	<b>10</b>
<b>Schedule 2 - Call-Off Contract charges</b>	<b>23</b>
<b>Part B - Terms and conditions</b>	<b>25</b>
<b>Schedule 3 - Collaboration agreement</b>	<b>45</b>
<b>Schedule 4 - Alternative clauses</b>	<b>45</b>
<b>Schedule 5 - Guarantee</b>	<b>45</b>
<b>Schedule 6 - Glossary and interpretations</b>	<b>45</b>
<b>Schedule 7 - Processing, Personal Data and Data Subjects</b>	<b>55</b>

## Part A - Order Form

<b>Digital Marketplace service ID number:</b>	333594048092159
<b>Call-Off Contract reference:</b>	Project 21878
<b>Call-Off Contract title:</b>	O365 Support and Professional Services
<b>Call-Off Contract description:</b>	The Supplier will deliver the technical support remotely from a UK Centre, this should deliver Infrastructure Operational Incident & Problem support. It will provide 24 x 7 support utilising leveraged services support teams included but not limited to Event Management, Major Incident Management & Technical Operations
<b>Start date:</b>	1 <sup>st</sup> July 2019
<b>Expiry date:</b>	30 <sup>th</sup> June 2021
<b>Call-Off Contract value:</b>	The initial Order Form value is £670,830.00 (exclusive of VAT), however the Parties reserve the right to uplift this Call-Off Contract by Variation up to a value of £4,000,000 (exclusive of VAT).
<b>Charging method:</b>	Monthly, in arrears
<b>Purchase order number:</b>	TBC following signed contract

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

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

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

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

<b>From: the Buyer</b>	<p>Department for Work and Pensions  Buyer's main address:  Caxton House  Tothill Street, Westminster  London  SW1H 9NA</p> <p>Buyer's Invoice Address:  Department for Work and Pensions  PO Box 406  SSCL  Phoenix House,  Celtic Springs Business Park  Newport  NP10 8FZ</p> <p>Electronic Invoices to be sent to APinvoices-DWP-U@sscl.gse.gov.uk</p>
<b>To: the Supplier</b>	<p>QBit Kloud Limited  Tel: 0203 882 0545  Supplier's address:  4 Christopher Street  London  EC2A 2BS  Company number:  09905640</p>
<b>Together: the 'Parties'</b>	

#### Principle contact details

<b>For the Buyer:</b>	[REDACTED]
<b>For the Supplier:</b>	[REDACTED]

## Call-Off Contract term

<b>Start date:</b>	This Call-Off Contract Starts on 1st July 2019 and is valid for 24 months
<b>Ending (termination):</b>	The notice period needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for disputed sums or at least 30 days from the date of written notice for Ending without cause.
<b>Extension period:</b>	This Call-Off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 4 weeks written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

## Buyer contractual details

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

<b>G-Cloud Lot:</b>	This Call-Off Contract is for the provision of Services under: Lot 3 - Cloud support
<b>G-Cloud services required:</b>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <p>Technical service providing 24/7 L3 to L3.5 support to resolve complex incidents, problems and changes with the option of onsite assistance and professional services.</p> <p>Sized at :</p> <p>10 technical Incidents per month</p> <p>Estimate 4 Problem per Month</p> <p>Estimate 2 Changes per Month</p> <p>With the option to go over this number on a cost per incident, problem and change basis and to have onsite support and professional services (see the pricing table).</p> <p>Access to a rich knowledge library or knowledge articles.</p>
<b>Additional services:</b>	N/A
<b>Location:</b>	The Services will be delivered to: Predominately Leeds and Newcastle but may include Manchester and London
<b>Quality standards:</b>	The quality standards required for this Call-Off Contract are stated in Schedule 1.

Technical standards:	The technical standards required for this Call-Off Contract are: ITIL Microsoft Gold Partner																
Service level agreement:	<p>The DWP will use Service levels to measure the performance of Service. Service Levels will be measured within the Authorities TechNow tool. The Supplier will also provide SLA reporting from their tool.</p> <p>The supplier will provide a 24 x 7 x 365 service desk, all manned by (FTE’s) to resolve complex incidents, problems and changes. The core Service Desk hours are 07:00 – 19:00 with support personnel situated within the Fordway offices in Godalming. Outside these hours the P1 &amp; P2 calls are handled by their out-of-hours team.</p> <p>Any of the Authorities teams can be part of the support process and get involved in the resolution. The supplier would always own and manage the calls (once they have been passed to the supplier by the agreed method). Should DWP wish to be part of the support process on an incident where this is going to impact on the SLA, DWP and the supplier can agree to either reduce DWP involvement to protect the SLA or to breach the SLA with DWP approval for that incident. It is DWP’s focus to improve its capability and to operate as proactively as possible so it may decide to breach an SLA on an incident in order to improve it’s understanding for future incidents.</p> <p>All calls will be handled by the suppliers 24x7 Service Desk, which is maintained between a day shift (07:00-19:00) and a night shift (18:00-08:00), which will cover the DWP required schedule. Their standard support is covered from 0700 to 1900 with P1’s and P2’s covered 24/7. There is no additional uplift in cost per incident for out of hours calls/incidents. The SLA’s for this Call-Off contract are:</p> <p><b><u>SLA’s in core hours</u></b></p> <table><tr><th>Priority</th><th>Definition</th><th>Response</th><th>Resolution</th></tr><tr><td>1</td><td>Critical systems outage affecting all or a substantial number of users. Typically failure of business critical servers, device or application, resulting in service unavailable to client</td><td>15 minutes</td><td>4 hours</td></tr><tr><td>2</td><td>Non-critical systems or service outage affecting a significant number of users. Limited or reduced service available to client.</td><td>1 hour</td><td>8 hours</td></tr><tr><td>3</td><td>Non-critical systems or service outage affecting one or a small number of users</td><td>4 hours</td><td>1 day</td></tr></table>	Priority	Definition	Response	Resolution	1	Critical systems outage affecting all or a substantial number of users. Typically failure of business critical servers, device or application, resulting in service unavailable to client	15 minutes	4 hours	2	Non-critical systems or service outage affecting a significant number of users. Limited or reduced service available to client.	1 hour	8 hours	3	Non-critical systems or service outage affecting one or a small number of users	4 hours	1 day
Priority	Definition	Response	Resolution														
1	Critical systems outage affecting all or a substantial number of users. Typically failure of business critical servers, device or application, resulting in service unavailable to client	15 minutes	4 hours														
2	Non-critical systems or service outage affecting a significant number of users. Limited or reduced service available to client.	1 hour	8 hours														
3	Non-critical systems or service outage affecting one or a small number of users	4 hours	1 day														

	<b><u>Incident Management Out of Hours Support</u></b>			
	<b>Priority</b>	<b>Definition</b>	<b>Response</b>	<b>Resolution</b>
	1	Critical systems outage affecting all or a substantial number of users, typically failure of business critical server, device or application, rendering service unavailable to client.	15 minutes	4 hours
	2	Non critical systems outage affecting a significant number of users; limited or reduced service available to client.	1 hour	8 hours
<b>Onboarding:</b>	The onboarding plan for this Call-Off Contract is stated in Schedule 1			
<b>Offboarding:</b>	N/A			
<b>Collaboration agreement:</b>	N/A			
<b>Limit on Parties' liability:</b>	<p>The annual total liability of either Party for all Property defaults will not exceed [REDACTED].</p> <p>The annual total liability for Buyer Data defaults will not exceed [REDACTED] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability for all other defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>			
<b>Insurance:</b>	<p>The insurance(s) required will be:</p> <p>A minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</p> <p>Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of [REDACTED] for each individual claim or any higher limit the Buyer requires (and as required by Law)</p> <p>Employers' liability insurance with a minimum limit of [REDACTED] or any higher minimum limit required by Law</p>			
<b>Force majeure:</b>	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 20 consecutive days.			
<b>Audit:</b>	<p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits.</p> <p>In accordance with clauses 7.3 to 7.12 of the Framework Agreement.</p>			
<b>Buyer's responsibilities:</b>	<p>The Buyer is responsible for providing the below details as applicable to that incident/problem/change:</p> <ul style="list-style-type: none"> <li>Providing adequate details of the incident, problem, change.</li> </ul>			

	<ul style="list-style-type: none"> <li>• DWP's system-generated incident/Problem/Change number.</li> <li>• Contact details of the person who is calling the supplier and owns the incident, problem or change within DWP.</li> <li>• Detail of the Technical Service impacted and any relevant sub-components impacted by the incident, problem or change.</li> <li>• The affected business service, if applicable.</li> <li>• The affected CI, if applicable.</li> <li>• The effect that the task has on business (if known).</li> <li>• A brief description of the incident, problem or change.</li> <li>• Detailed explanation on the incident, problem or change.</li> <li>• Sharing of contact means/media and escalation contacts where applicable.</li> </ul>
<b>Buyer's equipment:</b>	N/A


### Supplier's information

<b>Subcontractors or partners:</b>	<p>The following is a list of the Supplier's Subcontractors or Partners</p> <p>Fordway Limited  Hambledon House  Catteshall Lane  Godalming  Surrey  GU7 1JJ</p> <p>Tel: 01483 528200</p>
------------------------------------	---

### Call-Off Contract charges and payment

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

<b>Payment method:</b>	The payment method for this Call-Off Contract is BACS
<b>Payment profile:</b>	The payment profile for this Call-Off Contract is monthly in arrears.
<b>Invoice details:</b>	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
<b>Who and where to send invoices to:</b>	<p>Buyer's Invoice Address:</p> <p>Department for Work and Pensions</p>

	PO Box 406 SSCL Phoenix House, Celtic Springs Business Park Newport NP10 8FZ  Electronic Invoices to be sent to <a href="mailto:APinvoices-DWP-U@sscl.gse.gov.uk">APinvoices-DWP-U@sscl.gse.gov.uk</a>
<b>Invoice information required</b> – for example purchase order, project reference:	All invoices must include the purchase order and breakdown or charges
<b>Invoice frequency:</b>	Invoice will be sent to the Buyer monthly
<b>Call-Off Contract value:</b>	The initial Order Form value is £670,830 (exclusive of VAT), however the Parties reserve the right to uplift this Call-Off Contract by Variation up to a Call-Off Contract value of £4,000,000 (exclusive of VAT).
<b>Call-Off Contract charges:</b>	<p>The breakdown of the Charges is</p> <p>£198,000 pa for the technical service. In the rare event that an incident, problem, change cannot be resolved remotely an estimated £14,880 pa for onsite visits.</p> <p>See the rate card schedule 2 for full details.</p> <p>All expenses will be in accordance with the Buyer expense policy below:</p> <p> DWP Policy on Expenses for Business</p>

#### Additional buyer terms

<b>Performance of the service and deliverables:</b>	N/A
<b>Guarantee:</b>	N/A
<b>Warranties, representations:</b>	N/A
<b>Supplemental requirements in addition to the Call-Off terms:</b>	N/A
<b>Alternative clauses:</b>	N/A
<b>Buyer specific amendments</b>	N/A



<b>to/refinements of the Call-Off Contract terms:</b>	
<b>Public Services Network (PSN):</b>	N/A
<b>Personal Data and Data Subjects:</b>	Will Schedule 7 – Processing, Personal Data and Data Subjects be used - Yes

## 1. Formation of contract

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

## 2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.10.
- (B) The Buyer provided an Order Form for Services to the Supplier.

<b>Signed:</b>	Supplier	Buyer
<b>Name:</b>	[REDACTED]	[REDACTED]
<b>Title:</b>	UK Managing Director	Associate Commercial Specialist
<b>Signature:</b>		
<b>Date:</b>	6 <sup>th</sup> June 2019	7 <sup>th</sup> June 2019

## Schedule 1 - Services

### 1.1 Overview

The DWP requires a technical support service for services deployed within DWP for example On Premise Hosting and Azure environments. In addition, there is a requirement to provide ad-hoc support e.g. to enable the upgrade of future releases as well as security (and non-security type) updates of the products.

The DWP's applications such as Exchange Hybrid, Azure Active Directory (AAD) and New Technology File System (NTFS) are hosted within their data centre operations, with the Office Applications being hosted in the Microsoft Azure Cloud. Infrastructure are based across two sites, Corsham and Farnborough. The Microsoft Cloud is hosted in Microsoft's UK datacentre. All the applications are detailed in section 2.1 below.

The Supplier will provide 24 x 7 support utilising leveraged services support teams. They will engage and work with the DWP's level 3 support desk and also the DWP's Service Management, Technical Service teams, as well as other third parties employed by the DWP whilst providing the Service on an adhoc basis when dealing with Incidents, Problems and Changes.

The Supplier will provide a technical capability at an application level (above the OS) break/fix upon our hosted servers and Azure hybrid cloud services. The Supplier will offer typical in-house leveraged operational ITIL service management functions, to support the delivery of Services.

Technical support may be delivered by different technologies depending on the situation. For example, direct questions can be addressed using telephone calls or via E-mail. All incidents, problems and changes raised with the supplier will be logged and managed through a service management tool, that meets the DWP's security requirements.

Basic software problems can be addressed over the telephone. However, there may be a requirement for the Supplier to use remote access repair services into the authorities data centre.

Self-help is key to the DWP's user experience strategy, the Supplier will provide access to a rich library of technical support solutions to users relating to the applications listed below.

The Supplier should be a Microsoft Certified Partner and Global Solution Provider for Service Delivery and Support. They should be able to show technical competency in the technologies outlined in 'Schedule 1, 3.1 The Applications'

#### 1.1.1 Overview of the service to be provided by the supplier

The service will be provided by QBit Kloud in partnership with Fordway.

The services by the supplier, will adhere to ITIL v3 standards, follow ISO20000/27001 quality standards, utilising SC cleared SME resources. DWP will be the sponsoring organisation, for gaining SC clearance, for the supplier's staff if needed. Any financial cost relating to SC clearance to be borne by the supplier.

Both QBit and Fordway are Microsoft Gold Partners, holding both Gold Datacenter and Gold Cloud Platform competencies. In addition to the competencies at a company level, their team of consultants & SME's hold a wide variety of certifications including MCM, MCSE and MCSA in Microsoft technologies, assuring DWP that the supplier has the capability to deliver best practice Microsoft solutions and technical support on a variation of online, on-premise and Hybrid technologies and applications.

The supplier utilises Microsoft Advanced Support for Partners to assist it in providing its technical service to DWP. This can be leveraged to deliver escalation into Microsoft, and replace DWP's own "Premier Support Agreement" e.g. by DWP choosing to log their Microsoft calls via this contract rather than their own Premier Support Agreement.

Fordway is a Tier-1 Cloud Solution Provider, a program that means as a trusted advisor they can own the whole process of support from the beginning through to resolution, which means DWP will have one single point of contact from start to finish.

All Service Desk team members are permanent, full time employees of Fordway and have successfully completed and passed DBS / BPSS checks. As this is level 3/ L3.5 support, calls will go straight to their Security Cleared consultants.

### **1.1.2 Office 365 Technical Support Service**

The Supplier will deliver technical support remotely from a UK Centre. This will deliver Infrastructure Operational Incident, Problem and Change support. It will provide 24 x 7 support utilising leveraged services support teams included but not limited to Major Incident Management & Technical Operations.

The Supplier will provide Level 3-3.5 technical Support:

**Level 3** (abbreviated as L3) is responsible for handling complex or advanced incidents, problems and changes. It denotes expert level troubleshooting and analysis methods. It is typical for a developer or someone who knows the code or backend of the product, to be a level 3 support person. They will be an expert in the applications they will be supporting on behalf of the DWP. They are responsible for not only assisting L3 personnel, but with the research and development of solutions to new or unknown issues that DWP L3 cannot resolve.

For problem management the supplier will formulate and evaluate courses of action in a test case environment, and implement the best solution to the problem. Once the solution is verified, it is delivered in to DWP and made available for future troubleshooting and analysis.

The Supplier will provide information, a knowledge library or knowledge articles that will support Level 3/3.5 knowledge. This will benefit the Supplier and DWP in ensuring incident resolution moves to the left to reduce cost and increase service availability.

The supplier level 3.5 staff may not have direct access to DWP's environment. For security and effectiveness, supplier staff will require a DWP L3 support technician to facilitate access to their systems through a screen sharing solution. A screen sharing solution will be introduced, but as an interim solution screen shots will be shared. DWP reserve the right to introduce direct access to the systems.

All information of tickets will be recorded and logged to review in monthly service review meetings.

## 1.2 The Applications

The Applications, software and hardware at time of service enablement that the Supplier will be supporting are shown below. The Supplier will ensure that they have the necessary technical resource to provide L3.5 support for the following:

- Office 365
- SharePoint Online
- NTFS SAN Storage
- Visio
- Cisco Threat Management
- Veritas Netbackup
- Exchange
- Exchange online
- Office ProPlus
- Skype for Business Online and Hybrid
- MS Project
- Symantec Encryption
- Cisco IronPort
- Veritas Enterprise Vault
- Exchange Hybrid
- Power BI

Additional products can be added to the list at no additional cost as long as the supplier has the skills to cover the products. The list of qualifications held by the supplier and partner are shown below. If the total number of incidents, problems and changes go over the standard amount (10, 4 and 2) then the incident, problem, change will be costed for individually as per the costings in Schedule 2.

### No of FT technical staff per accreditation

- 8 x PRINCE2 practitioners, 7 other staff hold PRINCE2 Foundation
- 5 x ITIL consultants (2 Manager, 3 Practitioner), 34 other staff hold Foundation
- 8 x VMware Certified Professional
- 4 x Microsoft MCM's (Certified Masters)
- 36 x Microsoft MCSE, of which 18 have relevant Azure certifications including, 6 x Cloud Platform and 12 x Cloud Platform and Infrastructure, 23x MCIP, 28x MCP, 7x MCTS, 26x MCSA
- 4 x AWS Certified Cloud Practitioner, 2 x AWS Certified Solutions Architect, 1 x AWS SysOps Administrator
- 8 x Dell Compellent accredited installation and support engineers

- 4 x Dell Server installation engineers
- 2 x Certified EMC Networker Specialists
- 5 x Certified Commvault Certified Architect/Installation specialists
- 3 x Veritas NetBackup Certified Engineers / 2 x Veritas Enterprise Vault accredited
- 4 x Quest vWorkspace
- 3 x Cisco CCIE, 3 x Cisco CCNP, 5 x Cisco CCNA/CCDA/CCSE
- 3 x HP Openview accredited / 7 x HP ASE for Intel based servers and Blade Centre
- 3 x HP Procurve accredited / 2 x HP StorageWorks qualified
- 3 x HDS accredited installation and support engineers
- 3 x Red Hat Certified Engineers / 4 x Sun STK disk and tape accredited engineers
- 2 x Citrix CCSE
- 4 x Check Point certified / 3 x CISSP

### 1.3 Knowledge and capability

The supplier will provide DWP with knowledge articles pertaining to the products they are supporting for/with DWP. These will be designed to provide hints and tips, with documentation on how to resolve commonly known issues. The supplier encourages customers to use this, as often the answer can be found here and can save the service desk from being contacted.

At the end of each resolution the supplier will provide full details on how it resolved the issue so that DWP can build out it's own capability. If required by DWP there will be a call with the supplier (soon after resolution) so that DWP can clarify their understanding of the resolution steps and work arounds, in order to create a knowledge article where none is provided by the supplier.

### 1.4 Service support operation

#### 1.4.1 Incident and problem management

**An incident** is an event that could lead to loss of, or disruption to, an organization's operations, services or functions. The Supplier will complete Incident management of the applications it supports on behalf of the DWP. The Supplier will aim to identify, analyse, and correct hazards to prevent a future re-occurrence. Incident management should aim to limit the potential disruption caused by such an event, followed by a return to business as usual. Without effective incident management, an incident can disrupt business operations,

The Supplier will record incidents within a toolset and complete analysis to identify potential improvements to the service to reduce the number of incidents raised into the L3 relating to the applications supported by the Supplier. The supplier will provide a work around where possible to return service to normal whilst continuing to find a solution to the underlying issue.

**Problem:** The Supplier will support the identification and resolution of problems related to the applications being supported. Problem Management includes the activities required to diagnose the root cause of incidents identified through the Incident Management process, and to determine the resolution to those problems. The Supplier will also be responsible for ensuring that the resolution is implemented through the appropriate control procedures, especially Change Management and Release Management.

Using a service management issue logging toolset the Supplier will maintain information about problems and the appropriate workarounds and resolutions, so that the DWP is able to reduce the number and impact of incidents over time. The Supplier will interface with the Authorities Knowledge Management process by ensuring that resolution steps and work around are provided at the end of resolution so that a knowledge article can be developed where none is provided by the supplier or it is inadequate. Where clarification is needed there will be call between the supplier and DWP soon after the resolution. Although Incident Management and Problem Management are separate processes, they are closely related and will typically use the same tools, and may use similar categorisation, impact and priority coding systems. This will ensure effective communication when dealing with related incidents and problems.

#### 1.4.2 The DWP service model

Level of service	Incident management	Major incident management	Problem management	Change management
Level 0	User self-service with the use of knowledge articles	DWP UXCC team monitor DWP systems in On Premise Hosting and will raise a P1 call if there is an outage. They will get in touch with L3 and will decide if the DWP Major Incident Team is also needed.	-	-
Level 1	Third party service desk. They raise an incident in ServiceNow/Technow and resolve the majority of the incidents.	Will raise priority 1 call if they receive a call or call trend that warrants it. This will be flagged to UXCC who will contact L3.	-	-
Level 2	DWP service desk (based in Manchester)	Will raise priority 1 call if they receive a call or call trend that warrants it, This will be flagged to UXCC who will contact L3.	-	-

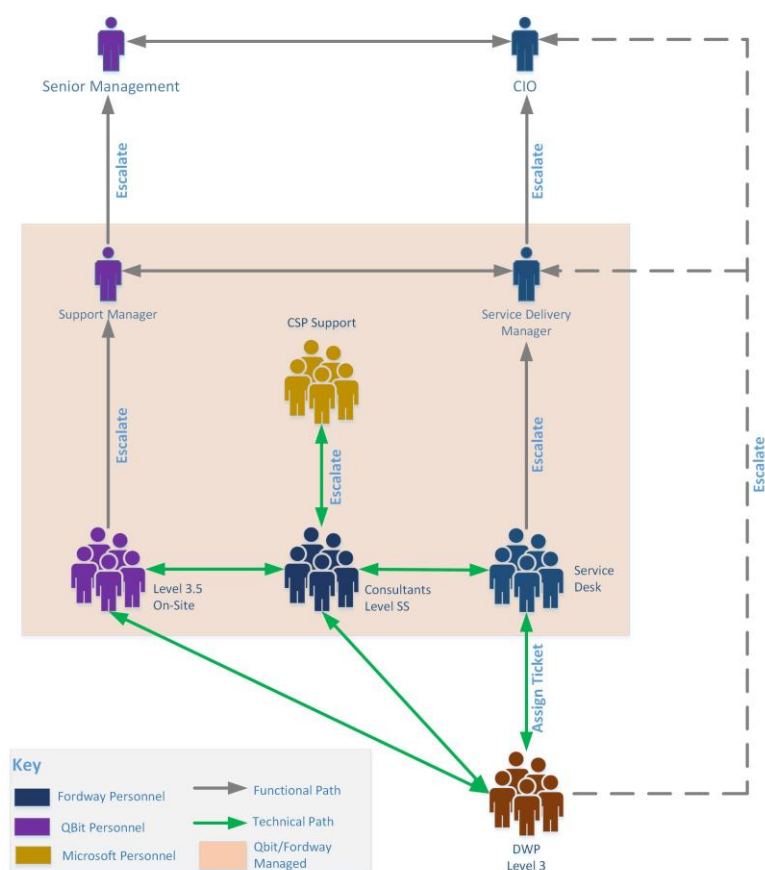
Level 3	DWP technical teams – low volume of incidents	Will raise priority 1 call if they receive a call or call trend that warrants it and assign to themselves. A P1 call will flag up to UXCC.	Problems are created at this level	Changes are created at this level
---------	---	--	------------------------------------	-----------------------------------

Incidents move through the levels i.e. if a user cannot resolve the issue themselves they contact level 1. If level 1 can't resolve the incident it is assigned to level 2, if they can't resolve then it goes to level 3.

### 1.4.3 The supplier service model

In the event that level 3 need assistance/resolution for an incident/problem/change or have more than they can handle, then they will contact the Supplier.

See the diagram below for the process the incident/problem will go through when assigned to the supplier.



### 1.4.4 Logging an incident/problem/change with the supplier

Incidents\Problems will be raised to the supplier service desk via telephone, email or their web portal.

When reporting a fault, the Supplier asks DWP to have the following information available when logging the call / raising the ticket:

- DWP ServiceNow/Technow incident/problem/change number
- Company name & contact details – name, phone, email
- What is the full nature of the incident, including systems/applications affected?
- What impact does this have on the business?
- When the issue was first noticed?
- Is the fault intermittent or permanent?
- Is this the first time this has occurred?

The supplier requires that when reporting a fault by email that it include “New Incident” in the subject line. This will auto generate a ticket within the Service Desk incident management tool.

DWP will provide their incident in the email for it to be captured in to the suppliers tool.

When DWP receive the suppliers number they will update their records with the number.

Correspondence about an existing incident is to include the suppliers IR number - issued by their Service Desk - in square brackets i.e. Re: [IR12345]. This will ensure that all email communication is recorded in the Incident ticket. Both numbers (suppliers and DWP) are to be used in all correspondence.

The supplier service Desk will be the SPOC for the DWP 3<sup>rd</sup> Line Support Teams. Outside of acting as the central point of contact the Service Desk will also perform the following activities:

- Receive all calls, chat request and e-mails on incidents
- Incident recording (including RFC's)
- Incident Classification (3rd Line / SS only)
- Incident Prioritisation including allowance for VIP's (Include P1's?)
- Incident Escalation to onsite / remote Security Cleared SME's
- Search for Work Around
- Update the customer and IT group on progress
- Perform communication activities for other ITIL processes (e.g. Release, Change, SLM-reports)
- Report to Management, Process Managers and DWP (through SLM) on Service Desk performance

Priority is assigned, and the incident is allocated to one of the Suppliers security cleared third line support SME's. Escalations and notifications are built into the workflow in the 'supplier service model' above. The supplier will have major incident workflows and security incident workflows (which includes data privacy streams).

#### **1.4.5 24/7 Onsite support**



In the event that an incident cannot be resolved remotely DWP will be given the option of an onsite visit. As this is at a cost (as per the costing in Schedule 2) a site visit will require prior approval and needs to be agreed with DWP before commencing. The supplier and its partner will organise the visit between them with DWP having the service desk as their single point of contact.

The site visit for P2 incidents will be next day, so long as the approval to proceed is agreed by 2pm on the day when the call was originally logged. P1 incidents will require best endeavours to attend site to DWP timescales at the earliest available opportunity. This may require a site visit to be made on a Saturday, Sunday or Bank Holiday, and the visit will start at 09:00 unless agreed otherwise with DWP.

#### **1.4.5.1 Management of onsite support costs**

The supplier partnership will use best endeavours to ensure that DWP are not charged for a remote incident, problem or change resolution and an onsite visit for the same incident, problem or change, as this would be doubling up the cost to DWP for a single resolution. It will always be the intention of the supplier partnership to ensure that only those incidents which cannot be resolved through remote triage and troubleshooting are escalated for approval to attend site at an additional fee – as outlined in the pricing schedule.

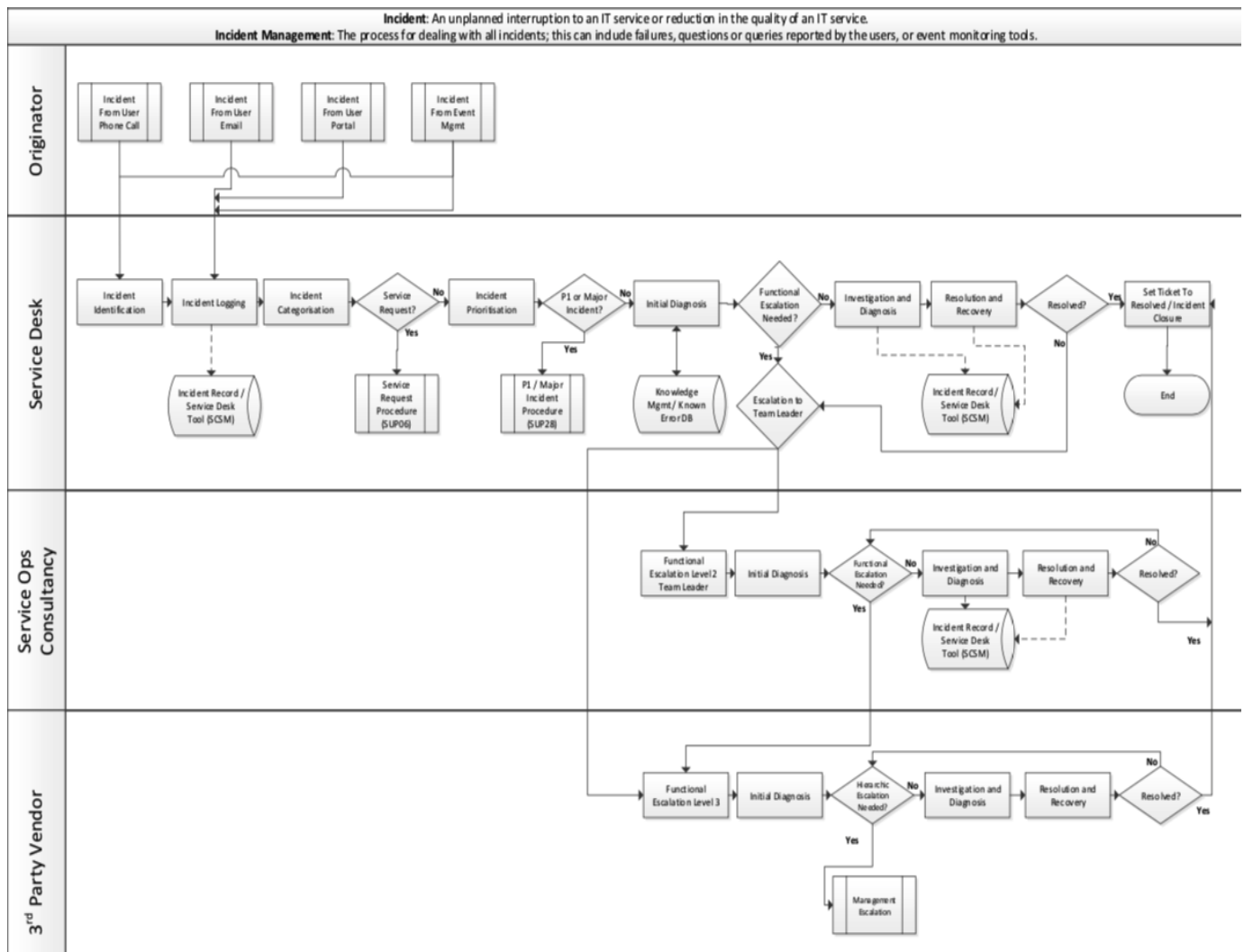
DWP will be supplied with a monthly report which correlates the incidents, problems and changes logged with those for which onsite visits were arranged. The report will make it clear which are being counted in the charging for remote resolution and are also being charged for an onsite day. These will be discussed in the monthly meetings to ensure that both the supplier and DWP understand the reasons and can determine any process improvements which would enable earlier identification of such in the future.

The supplier will also provide a cumulative report which shows all costs spent on this contract to date against the estimated spend as shown in Schedule 2 i.e. £198K for the service plus £14,880 for onsite visits and expenses. £14,880 is above the value DWP expect to spend as following the high percentage remote resolution rate achieved for the supplier's other customers it is anticipated that site visits will be rarely needed. Expenses for onsite visits will follow the DWP expense policy and will be based on actual cost up to a maximum of £250 per day.

Any disputes will follow the DWP dispute process.

#### **1.4.6 Escalation process**

Below is a diagram of the escalation process between Fordway and a customer, exact paths and roles will be defined between QBit, Fordway and DWP.



### 1.4.7 ITIL change management

DWP may wish to have assistance from the supplier with a change or hand over the change fully for the supplier to own.

#### 1) Change assistance

The Supplier will follow the Authorities standardised methods and procedures for efficient and prompt handling of all changes relating to the applications the supplier supports on behalf of the DWP. The aim is to minimise the number and impact of any related incidents upon service.

The Supplier will be expected to raise changes via the DWP's Service Now tool (if no access is granted then DWP L3 will complete this change record with information from the supplier). The supplier will be required to review changes that impact upon the applications and services that the supplier supports on behalf of the DWP. The supplier will be expected to support DWP by attending CABs as an SME where required.

## 2) Owning a change

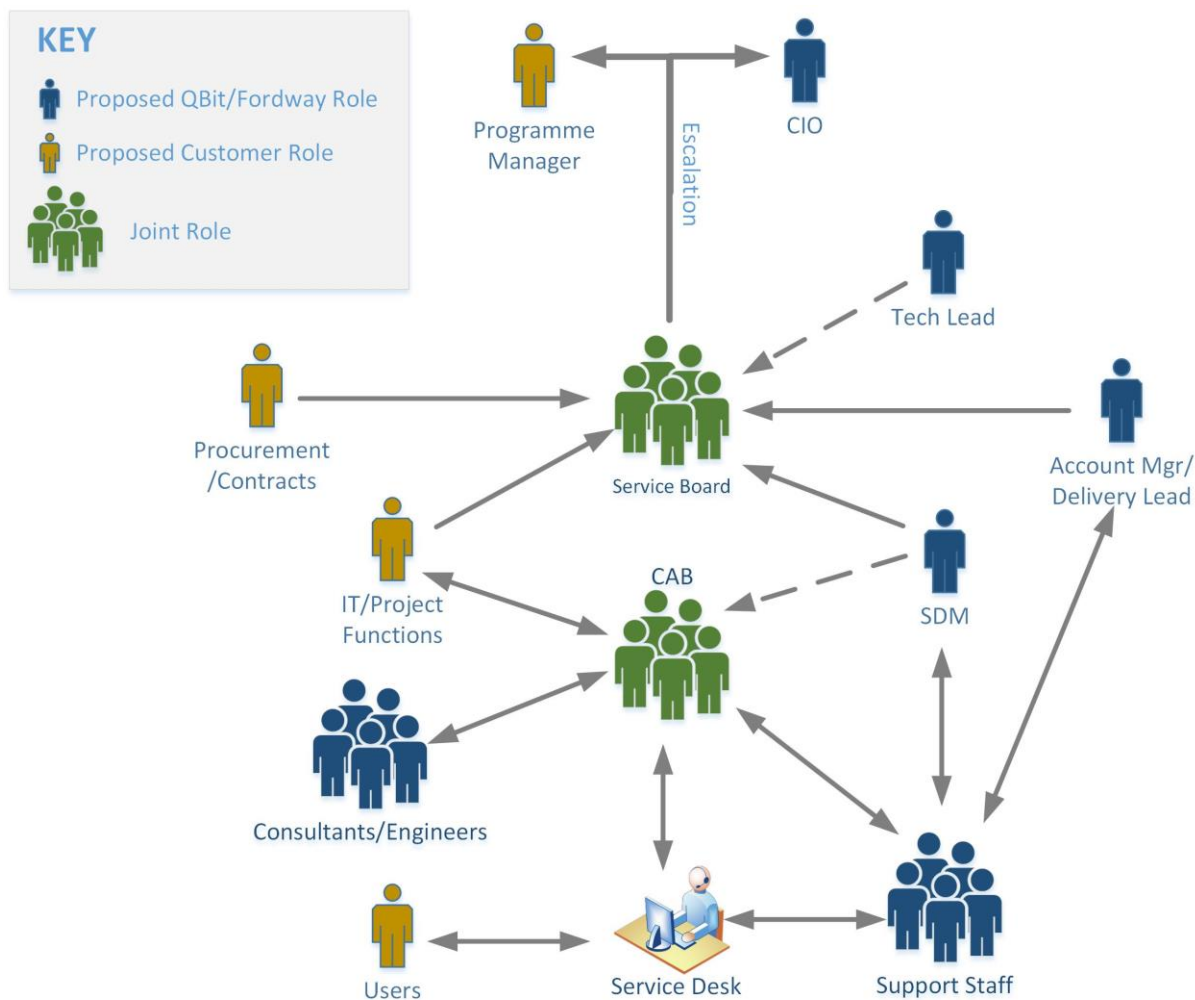
The Supplier will when requested by DWP own, define and recommend the change in question as part of either an Architecture or Operational change review board.

The attendees at the supplier CABs include the Service Desk, Service Delivery, Service Operations, Head of Technical & Operations, Security and Compliance Manager and a Change and Problem Manager. All appropriate change requests are referred to this board. Ultimate responsibility lays with the Suppliers Change and Problem Manager, who authorises any change requests and ensures that they are completed to the agreed SLA's. If required, and as outlined within the RFP, the supplier will work with DWP staff to support a specific CAB to discuss a change request.

Change Requests are logged, categorised and scheduled within the supplier Service Management toolset (SCSM) with appropriate implementation, test and risk inputs and approval mechanisms. The DWP change number and the Supplier's SCSM change number will be used in all correspondence relating to a change.

The supplier also has an Emergency Change procedure along with associated escalation and communication outputs.

Below is a diagram of the suppliers change management procedure.



## 1.5 Additional Project Delivery

From time to time DWP may wish to have a project delivered via this contract. The Supplier will provide different models to suit the types of delivery that DWP requires. For each project there will be a discovery engagement to identify which type of project will be utilised. This will develop a statement of works and is non-chargeable. This will be contracted as a variation. This variation will include details of:

- People
- Scope
- Outcomes
- Timescales
- It will have a termination notice period of 30 days

The costings will be as per the rates in Schedule 2 of this contract.

### **1.5.1 Project Specialist Technical Delivery**

DWP may require the Supplier to complete a small simple piece of Project Activity, such as drafting a technical design or configuration document. This will be the provision of a skilled individual to a specific requirement on a day rate charging basis. The DWP will be responsible for managing the individual and commercials, as well as the associated risk or reward if the project delivers quicker or slower than expected.

### **1.5.2 Project Adhoc Delivery**

DWP may wish to have project adhoc delivery. This would be a larger delivery, with a set of objectives and deliverables. The Supplier will scope out in partnership with the DWP a set of deliverables and produce a statement of work listing them and provide a commitment to deliver them. The delivery model will be based on actual work completed this a flexible resourcing model for Agile or DevOps projects.

### **1.5.3 Project Delivery fixed Outcome**

DWP may wish to have a fixed outcome project. This is suited to more complex projects where the deliverables and requirements are well understood and there is a need to ensure predictable cost. There is a thorough presales and requirements gathering activity conducted with DWP, after which a statement of work is produced which details the deliverables the Supplier will commit to. This will be utilised for larger transformation project such as user migrations.

### **1.5.4 Project mobilisation**

The Supplier will stand up a project team to implement the projects as per section 1.5 of this contract via a contract variation. The project will be led by a statement of works which will formalise the delivery of the new supplier support service and professional services.

The Project team will be dedicated to the delivery of this project and produce typical project collateral that will ensure quality, time and cost meet the DWP's expected levels.

The project will offer a warranty period to ensure that the project has delivered its expected deliverables until it is accepted into live by the DWP.

The project team will supply DWP with updated plans and reports as the project progresses at agreed points in time and when milestones have been achieved.

Where it applies the project stand up will be a fixed price piece of work based on delivery milestones.

## **1.6 General**

### **1.6.1 Account management**

An Account Manager, Delivery Lead and a Service Delivery Manager will be assigned to the DWP Account. Between them, they would triage any and all service, operational and project issues and be the primary point of contact. They will be responsible for ensuring the quality of service and will provide a monthly meeting a monthly reports.

### **1.6.2 Reporting schedule**

Monthly reports to include the following and delivered within 3 days of the end of the month:

No of incidents, problems and changes logged, type, priority, SLA and status.

A cumulative spend / utilisation report, which shows all costs spent on this contract to date against the estimated spend as shown in Schedule 2 i.e. £198K for the service plus £14,880 for onsite visits and expenses.

A report which correlates the incidents, problems and changes investigated remotely (counted in the costing figures) with those for which onsite visits were arranged.

### **1.6.3 Monthly meeting**

There will be a monthly meeting between DWP, QBit and Fordway. This may be done by a telephone, skype for business or face to face as agreed by the parties.

#### Typical agenda

- Run through the reports
- Discuss the costings
- Discuss service improvements – in particular where DWP have been charged for remote investigation into for any incidents, problems or changes which has not resulted in a resolution and has then required a chargeable day on site.

### **1.6.4 Service mobilisation**

If DWP utilise the service beyond the 10 incidents, 4 problems and 2 changes per month then the Supplier will expand their capacity to cope with the additional demand. It is anticipated that this could be increased 500% with no issues after which the supplier would quickly secure more resources to accommodate.

### **1.6.5 Security**

The supplier's controls need to meet the Authorities current security policies and processes. The supplier is to maintain its ISO9001, ISO14001, ISO20001, ISO27001, and its Cyber Essentials Plus certification.

The Suppliers staff need to have met the Authorities requirements for security vetting, with all staff used to deliver the authorities service to be Security Cleared. DWP will sponsor supplier members for security clearance. The associated costs will be borne by the supplier.

<https://www.gov.uk/guidance/security-vetting-and-clearance>

## **Schedule 2 - Call-Off Contract charges**

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract.

### **2.1 Technical service L3 to L3.5**

Below is the rate card to be used to cost the services in this contract.

There is a fixed fee element to retain the service and elements to cover 10 incidents, 4 problems and 2 changes per month. These elements are not based on a number of days. An incident may take 1 hour to fix or 2 days, either way it will be classed as one incident and will count towards the 10 incidents in that month.

There is also an amount for onsite visits and expenses.

**[REDACTED]**

Incident, problems and changes not utilised within the month will automatically roll over to the next month. The fixed volumes will be reviewed based on a rolling three-month basis.

Where an incident requires onsite support, the parties will jointly agree if this is deemed chargeable/ consumed as an incident.

Should DWP go over the number of incidents, problems or changes in a month then the additional will be costed as per the table below:

**[REDACTED]**

#### **2.1.1 Technical Innovation Days**

The supplier appreciates that DWP has contracted this service to manage its risk and that the service might be utilised sporadically during the term. As such in order to ensure a value-added return back to DWP the supplier will provide technical innovation days should DWP not use its full quota of monthly incidents (10) problems (4) and changes (2).

The days can be used for scoping out new solutions, technical training or hosting workshops to help drive the Digital Workplace agenda across DWP.

There will be a quarterly true-up of the service utilisation as outlined in the table below, which will then offer a quantity of Innovation Days which could be used anytime over the following 2 x quarters (6 months):

<b><i>Call Types p/Qtr</i></b>	<b>50-80% Utilisation</b>	<b>30-50% Utilisation</b>	<b>Up to 30% Utilisation</b>
<i>30 Incidents</i>	1 Innovation Day	2 Innovation Days	4 Innovation Days
<i>12 problems</i>			
<i>6 changes</i>			
<i>48 total in quarter</i>	If utilised 38 or less incidents, problems, changes in the previous quarter	If utilised 24 or less incidents, problems, changes in the previous quarter	If utilised 14 or less incidents, problems, changes in the previous quarter

N.B. Utilisation is measured across a combined view of all call types in the previous quarter.



## **2.2 24/7 Onsite Technical Days**

QBit Kloud have applied discounts of between 15%-30% have to the standard G-Cloud 10 Framework pricing. This matches the current rate DWP Office Productivity received from QBit resources under their our previous contract.

See 1.4.5 and 1.4.5.1 for details regarding the onsite technical days and how they should be managed. Below are the day rates depending on the level of resource needed to fix the issue.

Where on site presence is required this will be arranged as and when needed. Ability to get resource to site will be 1 working day from initial request.

Should it be identified that the supplier has sent an engineer to site incorrectly, they will refund DWP for that engineering cost or remove from the invoice.

**[REDACTED]**

## **2.3 On site professional services**

DWP estimate that they will require a number of SME's to fulfil statement of works briefed in Appendix 3 of this contract. The SME's are to produce outcome driven work – see Appendix 3. DWP anticipate that the SMEs will be needed for 6 months. The table includes an annual cost for completeness.

**[REDACTED]**

## **Part B - Terms and conditions**

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

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

## 2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.2 to 5.3 (Force majeure)
- 5.6 (Continuing rights)
- 5.7 to 5.9 (Change of control)
- 5.10 (Fraud)
- 5.11 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- a reference to 'CCS' will be a reference to 'the Buyer'

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

- 2.3 The Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.
- 2.4 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### **3. Supply of services**

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

### **4. Supplier staff**

- 4.1 The Supplier Staff must:
- be appropriately experienced, qualified and trained to supply the Services
  - apply all due skill, care and diligence in faithfully performing those duties
  - obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
  - respond to any enquiries about the Services as soon as reasonably possible
  - complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.
- 4.9 The Supplier will provide names of the people how may come to site so that DWP can check them for IR35 prior to them coming on site and being part of the resource for this contract.

## **5. Due diligence**

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

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

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

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

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

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

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

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

## **9. Insurance**

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
- during this Call-Off Contract, Subcontractors hold third-party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages,

including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of [REDACTED]

- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of [REDACTED] for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

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

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

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

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

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

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

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

## 10. Confidentiality

- 10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.83 to 8.91. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
- rights granted to the Buyer under this Call-Off Contract
  - Supplier's performance of the Services
  - use by the Buyer of the Services
- 11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
- modify the relevant part of the Services without reducing its functionality or performance
  - substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
  - buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

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

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

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

## **12. Protection of information**

12.1 The Supplier must:

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

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

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

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

## **13. Buyer data**

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

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

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



- 13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.
- 13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
- the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
  - guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Accreditation of Information Systems at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
  - the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/guidance/risk-management-collection>
  - government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
  - the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
- 13.6 The Buyer will specify any security requirements for this project in the Order Form.
- 13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

## **14. Standards and quality**

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

## **15. Open source**

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

## **16. Security**

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:

- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

- 16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

## **17. Guarantee**

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

## **18. Ending the Call-Off Contract**

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.
- 18.2 The Parties agree that the:
- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
  - Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses
- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any

unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
  - any fraud
- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
  - an Insolvency Event of the other Party happens
  - the other Party ceases or threatens to cease to carry on the whole or any material part of its business
- 18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
- 18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

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

- 19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.
- 19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.
- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- any rights, remedies or obligations accrued before its Ending or expiration
  - the right of either Party to recover any amount outstanding at the time of Ending or expiry

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

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

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

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

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

## 20. Notices

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

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

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

## 21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it. – See appendix for the Suppliers Exit Plan
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer

- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

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

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

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

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

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

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

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

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

## **23. Force majeure**

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

## **24. Liability**

- 24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:
- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
  - Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
  - Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

## **25. Premises**

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
- comply with any security requirements at the premises and not do anything to weaken the security of the premises
  - comply with Buyer requirements for the conduct of personnel
  - comply with any health and safety measures implemented by the Buyer



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

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

## **26. Equipment**

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

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

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

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

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

## **28. Environmental requirements**

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

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

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

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

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

- the activities they perform
- age

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

- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
- its failure to comply with the provisions of this clause
  - any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

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

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

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

### **31. Collaboration**

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

### **32. Variation process**

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

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

- 33.1 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only Processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional Processing if permitted by Law).
- 33.2 The Supplier will assist the Buyer with the preparation of any Data Protection Impact Assessment required by the Data Protection Legislation before commencing any Processing (including provision

of detailed information and assessments in relation to Processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.

- 33.3 The Supplier must have in place Protective Measures, details of which shall be provided to the Buyer on request, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.
- 33.4 The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier staff with access to Personal Data, including by ensuring they:
- i) are aware of and comply with the Supplier's obligations under this Clause;
  - ii) are subject to appropriate confidentiality undertakings with the Supplier
  - iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract
  - iv) are given training in the use, protection and handling of Personal Data.
- 33.5 The Supplier will not transfer Personal Data outside of the European Union unless the prior written consent of the Buyer has been obtained, which shall be dependent on such a transfer satisfying relevant Data Protection Legislation requirements.
- 33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.
- 33.7 The Supplier will notify the Buyer without undue delay if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation, and insofar as this is possible, in accordance with any timescales reasonably required by the Buyer
- 33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
- i) the Buyer determines that the Processing is not occasional;
  - ii) the Buyer determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
  - iii) the Buyer determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

33.9 Before allowing any Sub-processor to Process any Personal Data related to this Call-Off Contract, the Supplier must:

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

33.10 The Buyer may at any time put forward a Variation request to amend this Call-Off Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

### **Schedule 3 - Collaboration agreement**

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

### **Schedule 4 - Alternative clauses**

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

### **Schedule 5 - Guarantee**


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

### **Schedule 6 - Glossary and interpretations**

In this Call-Off Contract the following expressions mean:

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

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

<b>Commercially Sensitive Information</b>	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
<b>Confidential Information</b>	Data, personal data and any information, which may include (but isn't limited to) any: <ul style="list-style-type: none"> <li>● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above</li> <li>● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
<b>Controller</b>	Takes the meaning given in the Data Protection Legislation.
<b>Crown</b>	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
<b>Data Loss Event</b> 	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
<b>Data Protection Impact Assessment</b>	An assessment by the Controller of the impact of the envisaged processing by the Processor under this Call-Off Contract on the protection of Personal Data.
<b>Data Protection Legislation</b>	Data Protection Legislation means: <ul style="list-style-type: none"> <li>i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time</li> <li>ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy;</li> <li>iii) all applicable Law about the processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.</li> </ul>
<b>Data Subject</b>	Takes the meaning given in the Data Protection Legislation.

<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract</li> </ul> <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
<b>Deliverable</b>	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
<b>Digital Marketplace</b>	The government marketplace where Services are available for Buyers to buy. ( <a href="https://www.digitalmarketplace.service.gov.uk/">https://www.digitalmarketplace.service.gov.uk/</a> )
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: <a href="http://tools.hmrc.gov.uk/esi">http://tools.hmrc.gov.uk/esi</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.
<b>Force Majeure</b>	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:



	<ul style="list-style-type: none"> <li>● acts, events or omissions beyond the reasonable control of the affected Party</li> <li>● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>● acts of government, local government or Regulatory Bodies</li> <li>● fire, flood or disaster and any failure or shortage of power or fuel</li> <li>● industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure</li> <li>● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</li> </ul>
<b>Former Supplier</b>	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
<b>Framework Agreement</b>	The clauses of framework agreement RM1557.10 together with the Framework Schedules.
<b>Fraud</b>	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
<b>Freedom of Information Act or FOIA</b>	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.

<b>GDPR</b>	The General Data Protection Regulation (Regulation (EU) 2016/679).
<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK Government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government guidance and the Crown Commercial Service guidance, current UK Government guidance will take precedence.
<b>Indicative Test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information Security Management System</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
<b>Insolvency Event</b>	Can be: <ul style="list-style-type: none"> <li>● a voluntary arrangement</li> <li>● a winding-up petition</li> <li>● the appointment of a receiver or administrator</li> <li>● an unresolved statutory demand</li> <li>● a Schedule A1 moratorium.</li> </ul>
<b>Intellectual Property Rights or IPR</b>	Intellectual Property Rights are: <ul style="list-style-type: none"> <li>● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</li> <li>● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</li> <li>● all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>

<b>Intermediary</b>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>● the supplier's own limited company</li> <li>● a service or a personal service company</li> <li>● a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
<b>IPR Claim</b>	A claim as set out in clause 11.5.
<b>IR35</b>	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
<b>IR35 Assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
<b>Law</b>	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
<b>LED</b>	Law Enforcement Directive (EU) 2016/680.
<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.

<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement section 6 (What you report to CCS).
<b>Material Breach</b>	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
<b>New Fair Deal</b>	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
<b>Order</b>	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an Order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
<b>Personal Data</b>	Takes the meaning given in the Data Protection Legislation.
<b>Personal Data Breach</b>	Takes the meaning given in the Data Protection Legislation.
<b>Processing</b>	Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. 'Process' and 'processed' will be interpreted accordingly.
<b>Processor</b>	Takes the meaning given in the Data Protection Legislation.
<b>Prohibited Act</b>	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:

	<ul style="list-style-type: none"> <li>● induce that person to perform improperly a relevant function or activity</li> <li>● reward that person for improper performance of a relevant function or activity</li> <li>● commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
<b>Project Specific IPRs</b>	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory Body or Bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant Person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the Employment Regulations applies.
<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.

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

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

## **Schedule 7 - Processing, Personal Data and Data Subjects**

### **Subject matter of the processing:**

The data processing will involve a high level diagnostic of electronic information held by the Department for Work and Pensions and is a fundamental part of the Level3/4 Technical Engineering activities being undertaken.

### **Duration of the processing:**

The duration of contract services under this Order Form

### **Nature and purposes of the Processing:**

The nature of the processing is that the company will have access to DWP electronic information.

The intended purposes are to provide a detailed level of diagnostic capability into internal back-end infrastructure systems and engineering/ admin level access of DWP's current information systems landscape (messaging platforms, collaboration platforms, data volumes, currency; ownership, duplication; storage repositories; structuring; classification; security etc.)

The purpose of the processing is to improve the way the DWP's information systems are managed, supported and remediated as part of the digital transformation programme.

In some instances, the approach is governed in order to better comply with the law whilst also increasing business productivity. Therefore, it aligns with DWP's public task and legitimate interest.

### **Type of Personal Data:**

Because the company will have access to all electronic information contained on Network File Shares (NTFS) and SharePoint (and possibly even some business systems) they will have access to all types of personal data (including special category and law enforcement. However, the diagnostic is at a high level and therefore should be a very limited need to access specific personal data of individuals.

**Categories of Data Subject:**

Because the company will have access to all electronic information contained on Messaging Platforms, Network File Shares (NTFS) and SharePoint (and possibly even some business Systems) they are likely to have access to all types of data subject data.

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

There will be no transfer of personal or special category data from DWP to the company. All data analysed will remain under the control and security of DWP, the company are being given access to data to deliver the required engineering support.

**Appendix****Appendix 1 – Description of service levels**

**Level 0** (or self-help) is in the form of "wikis" or FAQs that allow for users to access and resolve information on their own rather than have to contact a local Helpdesk or Service Desk for resolution. As articulated below the Supplier will provide relevant information and knowledge to support the DWP in developing internal scripts and knowledge.

**Level 1** (abbreviated as T1 or L1) is the initial support level responsible for basic customer issues. It is synonymous with first-line support, denoting basic level technical support functions. The first job of a L1 specialist is to gather the customer's information and to determine the customer's issue by analysing the symptoms and figuring out the underlying issue. When analysing the symptoms, it is important for the technician to identify what the customer is trying to accomplish so that time is not wasted on attempting to solve an issue instead of a problem.

This level should gather as much information as possible from the end user. The information could be computer system name, screen name or report name, error or warning message displayed on the screen, any logs files, screen shots, any data used by the end user or any sequence of steps used by the end user, etc. This information needs to be recorded into the Service Now logging system and mandatory information has been defined by the Authorities Process areas. This information is useful to analyse the symptoms to define the problem or issue.

**Level 2** (abbreviated as T2 or L2) is a more in-depth technical support level than L1. The technicians are more experienced and knowledgeable on a particular product or service. Technicians in this realm of knowledge are responsible for assisting Tier 1 personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues. However, prior to the troubleshooting process, it is important that the technician review the work order to see what has already been accomplished by the T1 technician and how long the technician has been working with the particular customer. This team needs to collect information such as



program name that is failed or application name or any database related details (table name, view name, package name, etc.) or API names. These details are useful for Level 3.

If a problem is new and/or personnel from this group cannot determine a solution, they are responsible for raising this issue to the Level 3 technical support group.

**Level 3** (abbreviated as L3) is responsible for handling the more difficult or advanced incidents and problems. It denotes expert level troubleshooting and analysis methods. It is typical for a developer or someone who knows the code or backend of the product, to be the Tier 3 support person.

**Level SS** (Supplier Support abbreviated as SS)

The Supplier will be an expert in the applications they will be supporting on behalf of the DWP. They are responsible for not only assisting L3 personnel, but with the research and development of solutions to new or unknown issues that L3 cannot resolve.

In some instances, an issue may be so problematic to the point where development or changes are required, support from the application Supplier (for example Microsoft) will be requested and ownership will be given to the DWP to manage the incident through to resolution. If it is determined that a problem can be solved, this group is responsible for designing and developing one or more courses of action, evaluating each of these courses in a test case environment, and implementing the best solution to the problem. Once the solution is verified, it is delivered to the DWP and made available for future troubleshooting and analysis.

**Level 4**, the DWP will provide a fourth level. This represents an escalation point beyond the organisation. Level 4, is a Senior Product Design Engineer or Architect. The fourth level also represent the Research & Development of the products.

## **Appendix 2 – Supplier Exit Plan**

- QBit will receive formal notification to terminate the service from an authorised person.
- Date and time of expiration of the service will be agreed.
- Detail of data and applications to be returned to the Customer will be agreed. Customer to provide suitable hardware, media or other cloud service with sufficient capacity to migrate any agreed data.
- All relevant systems and services will cease at the allotted time.
- Any data and customer supplied application licences will be returned to the Customer.
- Once all data has been returned, and data held by QBit / Fordway's services on behalf of the Customer will remain available for 30 days after service termination, following this it will be deleted from Fordway's infrastructure in compliance with ISO27001 security procedures.

Any documentation created/used as part of the service, will be handed over. Depending on the systems/licences used to monitor/manage these will also be transferred. This may need manual transfer should systems not exist within the authority, therefore provided on a best efforts basis. Knowledge transfer and shadowing will be allowed during the exit period, however this is not training on tools/systems and assumes a reasonable level of competence by the person being shown the system.

Any IP ownership is included within the returning data, where appropriate.

Handover of operational activity will require the new providers to have sufficient capabilities to run/manage the necessary processes and systems, as stated above, we will provide assistance and explanations, however this does not include training people. It would be the up to the new provider to write their own procedures/processes or align to their systems.

The Supplier require a minimum of 30 days notice for termination of a service agreement.

### **Appendix 3 Job Descriptions & SOW Outcomes**

These are the outcomes for delivery from the SME resources.

#### **Statement of Work – Office Productivity – L3 Release and Packing Infrastructure Engineer : – Manchester and Leeds**

- Implement WSUS software deployment strategy for Apps and Office Clients
- For Office Clients develop SCCM Image build and deployment
- Develop OMS monitoring solution and trending to be pro-active with configuration of trending triggers with email injection into Service Now
- Investigate O365 Apps and develop troubleshooting and report gathering
- Office 365 Mobility - design, implementation and support BAU
- Support development of Systak – Office Client desktop enterprise monitoring solution
- Implement Client Apps Release Process
- Implement Evergreen Strategy
- Implement Office Client and O365 test process
- Configure Office and ProPlus Apps
- Test Office 365 Apps for to define future requirements

#### **Statement of Work – Office Productivity – Power BI - Leeds**

- developing a data pipeline to enable autonomous connection to dat sources
- maturing our analytics strategy through SME knowledge
- writing data queries to transform data preparation
- assisting with visualisation to help tell data stories and improve our products
- provide technical support in resolving power bi ETL issues/errors
- investigate new ways of working to increase data storage, ingestion and reporting

#### **Statement of Work – Office Productivity – - London**

- Implement SharePoint Online Search Centre
- Develop O365 Information Management (retention/review/disposal) solutions for gaps between E3 and E5 licence
- Developed/implementation of SharePoint Online ROI analytics

- Development of Azure services like AppSights for Analytics
- Configuration of Bot Framework platform to deliver the SharePoint Online bot
- Development of alternative or short term SharePoint Online site provisioning tools in case MIM is delayed
- Peer review of the Power Platform (Flow, PowerBI and Dynamics) and our security and governance settings
- Development of Power Platform PoCs inc Flow workflow solutions

#### **Statement of Work – Unified Communication – L3 Infrastructure Engineer : - Newcastle**

- Project Application development and implementation
- Skype Room System (SRS) design and build SRS endpoints sending out to 300 DWP destinations
- Understanding multiple site networks and communication rooms to assist and troubleshoot local related deployment issues
- Understanding of DNS and DHCP
- To work with Networks team assisting in troubleshooting F5 Proxy related issues
- To work with Networks team assisting in troubleshooting Palo Alto Layer 4 and Layer 7 multiple datacentre related issues
- WSUS software deployment strategy
- SCCM Image build and deployment
- Understanding of Skype Room System peripherals (Camera, Microphone, Display units)
- OMS monitoring solution and trending to be pro-active with configuration of trending triggers with email injection into Service Now
- Need to work with ServiceNow teams to understand the email injection from Azure Alerts to create identified incidents to be sent to correct teams to investigate
- O365 tenant experience with setting up Skype Room accounts and managing them through O365 Exchange and Skype Online
- O365 CQD understanding, troubleshooting and report gathering
- Skype Surface Hub - deployment and strategies with governance through O365
- Skype Mobility - design, implementation and support BAU
- Systak – Skype For Business desktop enterprise monitoring solution
- Design dashboard with a view to evolve as trending reports come in regarding issues seen
- Power BI
- Integrate OMS into Power-BI to have a combined same view for Services quick glance toolset
- Collaboration with Networks team – monitor DMZ and Network traffic between sites
- Collaboration with Office Productivity team against SME related Exchange issues

#### **Statement of Work – Unified Communication – L3 Infrastructure Engineer : - Newcastle**

- Configuration of Skype/Lync Hybrid integration with Skype for Business online | or Microsoft Teams

- Configuration of Exchange 2010/2013 Hybrid with Exchange Online in Office 365
- PowerShell Scripting for Migrating to Skype for Business Online (plus remote PowerShell to O365)
- Configuration and Troubleshooting of Azure AD Connect Directory Synchronization to office 365
- Understanding and Delivery of Active Directory Federation service for Office 365 integration for SSO.
- Leveraging Security Group based licencing model in Azure AD
- Securing O365 Global Admin accounts with Microsoft MFA
- Understanding of Target Proxy address and Alternate-ID proxy addressing process
- Reverse Proxy Experience - To publish Skype Web Services externally
- Internal and External DNS services troubleshooting.
- Remote PowerShell (Skype-connector | Azure | Exchange) to Office 365 services
- Replicate Policy and DLP configuration from On-Premise Lync or Skype to Skype for Business Online in O365
- Migration Pilot testing and Support
- Troubleshooting of Hybrid Audio and Video issues that crosses On-premise and Skype for Business Online in O365

### Example DWP JD



Job Description -  
Infrastructure Engineer