



Department for Education

G-Cloud 10 Call-Off Contract

Between

The Secretary of State for the Department for Education

And

Kainos Worksmart Ltd

For

Workday Implementation Services (HR, Payroll & Expenses)

Version 1.0 (Redacted)

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

Part A - Order Form	3
Schedule 1 - Services	22
Schedule 2 - Call-Off Contract charges	39
Part B - Terms and conditions	41
Schedule 3 - Collaboration agreement (Not Used)	61
Schedule 4 - Alternative clauses (Not Used)	61
Schedule 5 – Guarantee (Not Used)	61
Schedule 6 - Glossary and interpretations	61
Schedule 7 - Processing, Personal Data and Data Subjects	72
Schedule 8 – Additional Buyers Terms and Conditions	75
Annex 1	84

Part A - Order Form

Digital Marketplace service ID number:	108910173805379						
Call-Off Contract reference:	DfE Reference: Supplier Reference: Redacted						
Call-Off Contract title:	Workday Implementation and associated support services						
Call-Off Contract description:	The Supplier has been engaged by the Buyer to provide professional services for implementation of Workday and Workday support services.						
Start date:	4 th February 2019						
Expiry date:	3rd February 2021 (subject to the Customer electing to trigger the 1 year plus 1 year optional extensions under G-Cloud 10).						
Call-Off Contract value:	<p>The total potential contract value is Redacted (on the basis of the contact being extended in Year 3 (excluding expenses and VAT). The committed contract value is Redacted (for Years 1 and 2). The breakdown of the contract value is set out as follows:</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Estimated Cost (excluding Vat)</th> </tr> </thead> <tbody> <tr> <td>Implementation of Workday HCM, Payroll and Expenses</td> <td>Redacted Year 1 payment (Feb to March 19) = Redacted Year 2 payment (April 19 to Dec 19) Redacted</td> </tr> <tr> <td>Post-Deployment Support Application Management Service (AMS) (2 years)</td> <td>Redacted Year 1 payment (Dec 19 to March 20) = Redacted</td> </tr> </tbody> </table>	Item	Estimated Cost (excluding Vat)	Implementation of Workday HCM, Payroll and Expenses	Redacted Year 1 payment (Feb to March 19) = Redacted Year 2 payment (April 19 to Dec 19) Redacted	Post-Deployment Support Application Management Service (AMS) (2 years)	Redacted Year 1 payment (Dec 19 to March 20) = Redacted
Item	Estimated Cost (excluding Vat)						
Implementation of Workday HCM, Payroll and Expenses	Redacted Year 1 payment (Feb to March 19) = Redacted Year 2 payment (April 19 to Dec 19) Redacted						
Post-Deployment Support Application Management Service (AMS) (2 years)	Redacted Year 1 payment (Dec 19 to March 20) = Redacted						

	Year 2 payment (April 20 to Jan 21) = Redacted
	Estimated Total (Years 1 & 2) Redacted
	If the Buyer exercises its option to extend the Call-Off Contract in year 3, the estimated Charge for Post Development Support Application Management Service (AMS) will total Redacted
	For the avoidance of doubt, the Buyer is under no obligation to extend the Call-Off Contract beyond the initial 24 month term.
	Estimated Total (Years 1, 2 & 3) Redacted
The value above represents the full potential value of this Call-Off Contract.	
The actual committed contract value for the initial 24 month term is Redacted (excluding VAT).	
Charging method:	Time and Materials
Purchase order number:	TBC

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

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

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

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

From: the Buyer	THE SECRETARY OF STATE FOR EDUCATION whose Head Office is at Sanctuary Buildings, Great Smith Street, London, SW1P 3BT;
To: the Supplier	Kainos Worksmart Limited 02890 571100 Supplier's address: Kainos House, 4-6 Upper Crescent, Belfast, BT7 1NT Northern Ireland Company number: NI622516
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: Senior Contract Manager Name: Redacted Address: Sanctuary Buildings, Great Smith Street, London SW1P 3BT Email: Redacted Phone: Redacted
For the Supplier:	Title: WorkSmart Public Sector Lead Name: Redacted Email: Redacted Phone: Redacted

Call-Off Contract term

Start date:	This Call-Off Contract starts on 4 th February 2019 and is valid for 24 months.
--------------------	--

Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for disputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 1 month's written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud Lot:	This Call-Off Contract is for the provision of Services under: Lot 3 - Cloud support
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: Lot 3 - Cloud support The Supplier will provide professional services resource during the Workday Implementation of the HR, Payroll and Expenses functionality to carry out the services described in Parts A – E below during the Call-off Contract term, in accordance with the Implementation Methodology (www.kainos.com/wp-content/uploads/2014/12/Kainos-Workday-Implementation-Methodology_v4.0.docx .) and the assumptions and dependencies set out in it: Part A: 'Functional Scope' – as further detailed in Schedule 1 ; Part B: 'Integration Scope' – as further detailed in Schedule 1; Part C: Data Loads – as further detailed in Schedule 1; Part D: 'Worker Populations' – as further detailed in Schedule; Part E: 'Post Deployment Support Services' – as further detailed in Schedule 1. Workday automated testing SaaS, Smart™ ("Smart"). The Buyer has the option but not the obligation to procure Smart during the Call-off Contract term.

	<p>Details on the use and operation of Smart can be found in the Supplier’s Digital Marketplace entry here: https://www.digitalmarketplace.service.gov.uk/gcloud/services/829834516621460</p> <p>and in the Smart Terms of Use here: https://www.kainos.com/wp-content/uploads/2018/10/Kainos-Smart-Master-Subscription-Agreement-v4.0.pdf.</p> <p>The Buyer shall advise the Supplier’s principle contact, as set out above, should it wish to exercise its option to avail of Smart. The parties will use the G-Cloud Variation Process to contract the Smart option. The Smart Order Form is set out in Annex 1. Upon election of the option, this will be completed and executed as part of the Variation Process. The Order Form will stipulate the number of FSEs and the Smart module that the Buyer is wishes to procure.</p> <p>The charges for Smart have not been included in the Call-Off Contract value.</p>
Additional services:	N/A
Location:	<p>The Services will be delivered from:</p> <p>Suppliers sites: Belfast: 4-6 Upper Crescent, Belfast, County Antrim, BT7 1NT, U K; Dublin: 6-7 St Stephen’s Green, Dublin 2, Ireland; London: 4th Floor, 111 Charterhouse St, London, EC1M 6AW, U K; Gdansk: Tryton Business House, ul. Jana z Kolna 11, 80-864 Gdansk, Poland;</p> <p>To the Buyer’s sites: 2, St Pauls Place, 125 Norfolk St, Sheffield S1 2JF 20 Great Smith St, Westminster, London SW1P 3BT Piccadilly Gate, Store Street, Manchester, M1 2WD Or other Department of Education offices as advised</p>
Quality standards:	<p>The Supplier warrants that it will carry out the services with reasonable care and skill and that all services supplied hereunder shall be of satisfactory quality and fit for the particular purpose for which they are supplied with reference to the Customer's requirements and in line with G-Cloud 10 offerings</p> <p>The Supplier must confirm to the ISO 9001:2008 Quality Management System</p>

The quality standards specified within Service Requirements description outlined in Framework Section 2 will also apply.

Technical standards:

The technical standards required for this Call Off contract are:

- i) System security, availability and reliability maintained to ISO270001/20000-1/22301/27018 standards
- ii) Tool to remain compatible with current Microsoft software and Internet Browsers
- iii) Cyber Essentials accreditation
- iv) Compliance with accessibility standards W3C WA1: WCAG 2.0 AA level

Service level agreement:

The service level and availability criteria required for this Call-Off Contract, in relation to Post Deployment Support only are as follows:

Priority	Classification	Description & Examples	Target Response Time
Critical	High Impact & High Urgency	Business critical integration or software functionality not usable for any purpose; Data inaccuracies impacting all Workday users; All users affected; Unable to proceed and creating major business impact.	1 hour
High	High Impact & Medium Urgency; Medium Impact & High Urgency	Malfunction impacting important integration or software functionality; Business process, absence plan, benefits plan or similar isn't completing; Majority of users affected.	2 hours
Medium	High Impact & Low Urgency; Medium Impact & Medium Urgency Low Impact & High Urgency	Malfunction impacting standard integration or software functionality; Business process, absence plan, benefits plan or similar creating an issue, but workaround available; Multiple users affected.	4 hours
Low	Medium Impact & Low Urgency	Malfunction impacting non-critical integration or software functionality;	1 day

		Low Impact & Medium Urgency	Business process, absence plan, benefits plan or similar requires amending, but not blocking progress; Single user affected or multiple users inconvenienced.	
	Minor	Low Impact & Low Urgency	Minor issue inconveniencing users; No impact on business; Cosmetic modification; Usability suggestion.	2 days
	Query	Request for advice, guidance or information	Request for investigation into behaviour of functionality; Request for instructions or guidance on how to achieve outcome.	2 days
	Service Request	Standard change that does not require approval	Password reset; Set up of new KIM user.	2 days
	Problem	Investigation of underlying root cause of 1 or more Incidents	Grouping of one or more Incidents with similar symptoms to investigate and resolve underlying root cause.	2 days
	Change Request	Request for change or enhancement	Introduction of new functionality; Enhancement of existing functionality.	2 days
Onboarding:	<p>The onboarding plan for this Call-Off Contract is detailed in the Supplier Workday I Implementation Methodology: https://www.kainos.com/wp-content/uploads/2016/04/Kainos-Workday-Implementation-Methodology_v4.0.pdf</p> <p>The Buyer and Supplier shall attend a start-up meeting with representatives of the Buyer. At this meeting the agenda will include but not be limited to: discussion and agreement on activity to implement the service within the DfE,</p>			

	<p>future contract management arrangements; project documentation and deliverables; service delivery KPIs; requirements for reporting of Management Information consistent with clause 8 of the framework agreement (if any); and a forward schedule of meeting dates.</p> <p>As a minimum, the Supplier’s Account Manager for the DfE shall attend and fully participate in agreed contract and service review meetings chaired by the Buyer. The agenda for this meeting will be issued to participants at least three (3) working days in advance of the meeting and include a monthly Service Report produced by the Supplier. Frequency of meetings will be monthly, with the potential to increase should the service degrade / risk increase.</p> <p>The detailed content of the Service report shall include as a minimum: progress against delivery of implementation plan(s), forward and retrospective resource plan, risks and issues log, financial reporting, incidents and service failure log; quality assurance.</p>
Offboarding:	<p>The off-boarding plan for this Call-Off Contract will be developed by the Supplier and agreed between the Buyer and the Supplier within 6 months of the contract commencement date and reviewed 3 months prior to the end of the contract. As a minimum this will involve:</p> <ul style="list-style-type: none"> • Ensuring the transfer of knowledge to the Buyer, a representative nominated by the Buyer or a different Supplier, • Ensuring the return of any Data within agreed deadlines <p>Any offboarding requested by the Buyer, had not been included within the estimated costs and will be provided by the Supplier, at the G-Cloud rates, and charged on a time and materials basis.</p>
Collaboration Agreement	<p>Not applicable although it is recognised that the Supplier, in order to deliver the implementation, needs to collaborate and work in partnership with Workday the HR, Payroll and Expenses solution Provider. The Supplier must also fully engage and support Workday during their Delivery Assurance function whereby they undertake scrutiny and peer reviews at various stages within the implementation.</p>
Limit on Parties’ liability:	<p>The annual total liability of either Party for all Property defaults will not exceed £ 1,000,000.</p>

	<p>The annual total liability for Buyer Data defaults will not exceed £1 million or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Insurance:	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days
Audit:	The Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits.
Buyer's responsibilities:	The Buyer is responsible for the tasks outlined in the assumptions and dependencies sections above, the Supplier Workday Implementation Methodology and the Supplier's terms and conditions on the Digital Marketplace.
Buyer's equipment:	N/A

Supplier's information

Subcontractors or partners:	N/A
-----------------------------	-----

Call-Off Contract charges and payment

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

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

	<ul style="list-style-type: none"> • for Workday Implementation Services provided from the Start Date, up to and including the 29th March 2019 (“Initial Invoice Date”), the Supplier will invoice the Buyer on a time and materials basis, in line with the published rate card, for the sum of Redacted (plus VAT and expenses, as applicable) (the “Initial Payment”). • In the event that the Initial Payment is not utilised in full, before the Initial Invoice Date, any unused balance will be credited toward future invoices. • Subsequent invoices will be raised, monthly in arrears to reflect actual utilisation, in line with the published rate card. 				
Invoice details:	<p>The Supplier will issue electronic invoice, in line with the payment profile above.</p> <p>The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.</p>				
Who and where to send invoices to:	<ul style="list-style-type: none"> • Electronic invoices will be sent to: APinvoices-DFE-U@sscl.gse.gov.uk 				
Invoice information required – for example purchase order, project reference:	<p>A valid invoice is one that is:</p> <ul style="list-style-type: none"> • Is in an un-editable format such as pdf or jpeg • Delivered in timing in accordance of the contract and is not future dated • Is for the correct sum • Is correct in terms of services/goods supplied • Has a unique invoice number • Quotes a valid Purchase Order number • Includes correct supplier details, date, contact details • Valid Contract Number • Invoicing will be in £ Sterling <p>A copy invoice shall simultaneously be emailed to the DfE Buyer and the central mailbox Budgets.HRGrp@education.gov.uk to enable the Buyer to take receipting action</p>				
Invoice frequency:	Invoice will be sent to the Buyer monthly.				
Call-Off Contract value:	<p>Redacted (excluding expenses and VAT), which is set out as follows:</p> <table border="1" data-bbox="464 1666 1506 2004"> <thead> <tr> <th data-bbox="464 1666 999 1715">Item</th> <th data-bbox="999 1666 1506 1715">Estimated Cost (excluding Vat)</th> </tr> </thead> <tbody> <tr> <td data-bbox="464 1715 999 2004">Implementation of Workday HCM, Payroll and Expenses</td> <td data-bbox="999 1715 1506 2004"> <p>Redacted Year 1 payment (Feb to March 19)</p> <p>Redacted Year 2 payment (April 19 to Dec 19) = Redacted</p> </td> </tr> </tbody> </table>	Item	Estimated Cost (excluding Vat)	Implementation of Workday HCM, Payroll and Expenses	<p>Redacted Year 1 payment (Feb to March 19)</p> <p>Redacted Year 2 payment (April 19 to Dec 19) = Redacted</p>
Item	Estimated Cost (excluding Vat)				
Implementation of Workday HCM, Payroll and Expenses	<p>Redacted Year 1 payment (Feb to March 19)</p> <p>Redacted Year 2 payment (April 19 to Dec 19) = Redacted</p>				

	Post-Deployment Support Application Management Service (AMS) (2 years)	Redacted Year 1 payment (Dec 19 to March 20) = Redacted Year 2 payment (April 20 to Jan 21) = Redacted																									
	Estimated Total (Years 1 & 2)	Redacted																									
<p>If the Buyer exercises its option to extend the Call-Off Contract in year 3, the estimated Charge for Post Development Support Application Management Service (AMS) will total Redacted</p> <p>For the avoidance of doubt, the Buyer is under no obligation to extend the Call-Off Contract beyond the initial 24-month term.</p>																											
	Estimated Total (Years 1, 2 & 3)	Redacted																									
<p>The value above represents the full potential value of this Call-Off Contract.</p> <p>The actual committed contract value for the initial 24-month term is Redacted (excluding VAT).</p>																											
Call-Off Contract charges:	<p>The breakdown of the Charges is as set out below, the Charges are estimates and have been compiled on the basis of the assumptions and dependencies set out G-Cloud services required' section above:</p> <p>For the Workday Implementation Services (set out at Parts A-D in Schedule 1 below):</p> <table border="1" data-bbox="464 1429 1474 1930"> <thead> <tr> <th data-bbox="464 1429 809 1554">Role</th> <th data-bbox="809 1429 1032 1554">Man Day Rate (£)</th> <th data-bbox="1032 1429 1252 1554">Days</th> <th data-bbox="1252 1429 1474 1554">Estimated Total (£)</th> </tr> </thead> <tbody> <tr> <td data-bbox="464 1554 809 1630">Project Director</td> <td data-bbox="809 1554 1032 1630">Redacted</td> <td data-bbox="1032 1554 1252 1630">Redacted</td> <td data-bbox="1252 1554 1474 1630">Redacted</td> </tr> <tr> <td data-bbox="464 1630 809 1706">Engagement Manager</td> <td data-bbox="809 1630 1032 1706">Redacted</td> <td data-bbox="1032 1630 1252 1706">Redacted</td> <td data-bbox="1252 1630 1474 1706">Redacted</td> </tr> <tr> <td data-bbox="464 1706 809 1783">Data Consultant</td> <td data-bbox="809 1706 1032 1783">Redacted</td> <td data-bbox="1032 1706 1252 1783">Redacted</td> <td data-bbox="1252 1706 1474 1783">Redacted</td> </tr> <tr> <td data-bbox="464 1783 809 1859">HCM Lead Consultant</td> <td data-bbox="809 1783 1032 1859">Redacted</td> <td data-bbox="1032 1783 1252 1859">Redacted</td> <td data-bbox="1252 1783 1474 1859">Redacted</td> </tr> <tr> <td data-bbox="464 1859 809 1930">HCM Core Consultant</td> <td data-bbox="809 1859 1032 1930">Redacted</td> <td data-bbox="1032 1859 1252 1930">Redacted</td> <td data-bbox="1252 1859 1474 1930">Redacted</td> </tr> </tbody> </table>			Role	Man Day Rate (£)	Days	Estimated Total (£)	Project Director	Redacted	Redacted	Redacted	Engagement Manager	Redacted	Redacted	Redacted	Data Consultant	Redacted	Redacted	Redacted	HCM Lead Consultant	Redacted	Redacted	Redacted	HCM Core Consultant	Redacted	Redacted	Redacted
Role	Man Day Rate (£)	Days	Estimated Total (£)																								
Project Director	Redacted	Redacted	Redacted																								
Engagement Manager	Redacted	Redacted	Redacted																								
Data Consultant	Redacted	Redacted	Redacted																								
HCM Lead Consultant	Redacted	Redacted	Redacted																								
HCM Core Consultant	Redacted	Redacted	Redacted																								

Core Compensation Consultant	Redacted	Redacted	Redacted
Benefits and Absence Consultant	Redacted	Redacted	Redacted
Payroll Consultant	Redacted	Redacted	Redacted
Talent and Recruiting Consultant	Redacted	Redacted	Redacted
Expenses Consultant	Redacted	Redacted	Redacted
Learning Consultant	Redacted	Redacted	Redacted
Reporting Consultant	Redacted	Redacted	Redacted
Integrations Lead Consultant	Redacted	Redacted	Redacted
Integrations Consultant	Redacted	Redacted	Redacted
Allowance for Expenses			Redacted
Totals (£)		Redacted	Redacted

For the Post-Deployment Support Services (set out at Part E in the ‘G-Cloud services required’ section above):

The Post-Deployment Support Application Management Service (AMS) is provided on the basis of pre-paid Man Days at a discounted rate of **Redacted** per pre-paid Man Day (the “**Pre-Paid Man Day Rate**”).

Pre-Paid Man Days

The number of pre-paid Man Days have been profiled as follows (“**Pre-Paid Man Day Payment Profile**”):

- o Year 1 days required estimated at **Redacted** Man Days (Dec 19 to March 20);
- o Year 2 days required estimated at **Redacted** Man Days (April 20 to Jan 21);

and

Year 3 days required estimated at **Redacted** Man Days (Feb 21 to Jan 22).

Year 3 days are NOT included in the committed contract value and will only apply if agreement is given to extend the contract beyond the 2 year term.

- AMS is provided on a time and materials basis. The Supplier will not be responsible for the provision of AMS (or the consequences of failing to provide AMS) where there are no available pre-paid Man Days.
- All pre-paid Man Days must be used within the Call-off Contract Term or they will lapse.
- No refund or credit will be given at the end of the Call-off Contract Term for unused pre-paid Man Days.
- Additional pre-paid Man Days may be purchased at any time during the Call-off Contract Term via a Variation to this Call-off Contract.

Project Work

- The Pre-Paid Man Day Rate is for Post-Deployment Support Application Management Service (AMS).
- Buyer may request that the Supplier carries out Project Work under this Order Form by using the Change Request (CR) process. This will be coordinated centrally within the Buyers' HR team and only those CR's that have been signed off by a nominated Responsible Officer should be assessed by the Supplier. On receipt of a Change Request the Supplier will assess the work/resource required. Those that need less than five (5) days can proceed without a full assessment, those that need five (5) or more days will need to be reviewed by the Buyer before the work can commence.
- Where any individual or series of related Project Work exceeds 16 Man Days, is delivered by the AMS support team, and is within the scope of AMS, this will be drawn down against Pre-Paid Man Day Rate. Where any Project Work exceeds 16 Man Days and falls outside the normal scope of AMS or requires a change to the AMS staff profile, then the current SFIA rate card (and not the Pre-Paid Man Day Rate) will apply.

To fund agreed Project Work, the Buyer may either, via a Change Request to this Call-off Contract:

- use its available pre-paid Man Days (where the project work is less than 16 Man Days); OR

- use its available pre-paid Man Days (where the project work is more than 16 Man Days) paying the difference between the Pre-Paid Man Day Rate and the rate card Man Day rate; OR
- purchase additional Man Days for the Project Work at the rate card.

Total estimated Charges for Post-Deployment Support Application Management Service (AMS) over 2 years is **Redacted** (calculated according to the Pre-Paid Man Day Payment Profile above).

If the Buyer exercises its option to extend the Call-Off Contract in year 3, the estimated Charge for Post Development Support Application Management Service (AMS) will total **Redacted**

For the avoidance of doubt, the Buyer is under no obligation to extend the Call-Off Contract beyond the initial 24 month term.

Overtime & On-Call Support

Any time spent by the Supplier in the provision of the AMS outside the Service Hours and upon explicit request from the Buyer will be undertaken subject to the following provisions governing out-of-hours support.

Work to be undertaken outside the Service Hours (depending on its nature and duration) will be classified by the Supplier (in advance of it being undertaken) as either:

“Overtime” or "On-Call Support"

The standard Service Hours for AMS are: Monday to Friday 0900-1700 GMT
Excluding UK public holidays

Overtime will be charged at the Overtime Rate (see table below for rates).

On-Call Support comprises two charging elements:

- (a) A flat daily charge for the provision of the On-Call Support facility which will be billed at the “On-Call Daily Rate” set out in the Order Form plus VAT and expenses (if any); and
- (b) An hourly charge for each call made during an On-Call Support period which will be billed at the “On-Call Hourly Charging Rate” set out in the Order Form, per hour, plus VAT and expenses (if any).

Calls made during an On-Call Support period will be logged at a minimum of two (2) hours irrespective of their duration subject to the following:

(a) Once the two (2) hour minimum period has been triggered, the Buyer will not be charged for any additional calls made (if any) within that two (2) hour period;

(b) Where a call (or calls) exceed(s) the initial (2) hour period, or where additional calls are received after the initial two (2) hour period has expired then, , further time will be charged at a minimum of one (1) hourly increments, subject to the following:

Once the one (1) hour minimum period has been triggered, the Buyer will not be charged for any additional calls made (if any) within that one (1) hour period. In the event that more than one (1) hour has passed from the end of the last call received then the minimum call charge will revert to the standard two (2) hour minimum period.

Additional Rates

On-Call Rate for each Man Day of AMS coverage outside the Service Hours:	@ 0.5 x Pre-Paid Man Day Rate
On-Call Man Day Call Out Charging Rate:	@ 1.5 x Pre-Paid Man Day Rate
Buyer Requested Overtime Rates:	@ 1.5 x Pre-Paid Man Day Rate outside Service Hours @ 2 x Pre-Paid Man Day Rate weekend and public holidays

Expenses

Expenses will be charged at cost for services carried out at the Buyer's site following the below policy:

Travel – the Supplier must use low cost providers in purchasing flight, rail and road tickets to perform the Services at the Buyer place of business.

	<p>Restricted/Non-refundable ticket must be booked, no open tickets are allowable. For the avoidance of doubt travel time for the Supplier's personnel or representatives will not be incurred as a cost to the Buyer</p> <p>NB - Where the engagement is for a longer period of time and it makes commercial sense the Supplier may, with the Buyer's approval, procure rented accommodation.</p> <p>The above limits are for overnight accommodation required whilst the Supplier personnel are delivery the Services at the Buyers place of business. Any / all exceptions to the above must be raised and agreed in writing in advance with the Buyer.</p> <p>The Supplier shall work with the Buyer to minimise the impact on the public purse of travel and subsistence (“T&S”) associated with the operation of this contract. Unless otherwise provided for under the Supplier's G-Cloud 10 framework offering and/or the Supplier has an office in close proximity of the Buyers office where a meeting is to be held (approx. 25 miles radius), where expenditure on T&S is identified as being necessary for the effective operation of the contract, T&S will be paid at the level commensurate with the Buyer rate in place at the time the expenditure is incurred. DfE rates in place as at 1st January 2019 are listed below:</p> <ul style="list-style-type: none">• Hotel accommodation bed and breakfast – London £110.00 including VAT and elsewhere £75.00 including VAT• Rail travel shall be restricted to standard class• Car mileage at the ‘Public Transport Rate’ of 0.25p per mile• Taxis only payable where their use can be justified against using public transport <p>No other out of pocket expenses shall be allowable unless pre-approved with the Buyer.</p>
--	--

Additional buyer terms

Performance of the service and deliverables:	The performance of the Supplier will be measured using the following indicators and the targets monitored:			
	Indicator	Detail	Measurement	Target
	Effectiveness - Percentage of project milestones signed off on time	Are the different stages of the project being completed in a timely manner?	Percentage of total	90%
	Effectiveness - Number of change requests	Have the requirements been properly understood, ratified by the business and satisfactorily delivered?	Count of total	0
	Quality – ratio of defects	How frequently are we getting things wrong and having to rework them?	Ratio of development effort (days) versus defects raised	10
	Budget - Percentage of cost variance	How much does the actual cost vary from the projected cost?	Percentage of actual cost versus forecast cost	10%
	Timeliness - Percentage of tasks complete on time	How many tasks are completed by a given deadline?	Percentage of tasks complete on time versus total tasks	90%
<p>Within the scope of the Call-Off Contract, the Supplier will also:</p> <ul style="list-style-type: none"> • attend and participate in joint planning and delivery workshops chaired by the Buyer • work to an agile/waterfall/hybrid methodology; such as attend agile ceremonies and participate in delivering designated tasks. 				

	<ul style="list-style-type: none"> • provide specialist resources to QA / validate requirements on a periodic basis through elaboration and refinement sessions, as agreed with the Buyer; • author design documentation, which includes requirements traceability, to support development work as coordinated with the Buyer's technical representative • ensure coding standards are adhered to, as specified by the Buyer.
Guarantee:	N/A
Warranties, representations:	As per the Call -Off Contract.
Supplemental requirements in addition to the Call-Off terms:	<ul style="list-style-type: none"> • Within the scope of the Call-Off Contract, the Supplier will not be required to make the IPR of any Project IPRs or Third Party IPR open source.
Alternative clauses:	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms:	Within the scope of the Call-Off Contract, the Supplier will adhere to the Buyers Special Terms as set out in Schedule 8.
Public Services Network (PSN):	N/A
Personal Data and Data Subjects:	Will Schedule 7 – Processing, Personal Data and Data Subjects be used - Y

1. Formation of contract

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

2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.10.

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

Signed:	Supplier	Buyer
Name:	Redacted	Redacted
Title:	Head of Workday Business Units	HR Director
Signature:	<u>X</u>	<u>X</u>
Date:		

Schedule 1 - Services

The Supplier shall provide Lot 3 Cloud Support in accordance with the service definition “Workday Implementation Services” – Service ID 1089 1017 3805 379 of the Digital Market Place refers. This Service ID covers the following provisions:

Part A – Functional Scope

The Supplier will design and configure generally available functionality of Workday as prioritised by the Buyer. The configuration of each component listed below will be prioritised and designed during the early stages of the project. The listed processes are representations of key business processes to be designed and configured.

HCM:

- Organisation Structures – creating hierarchy of organisations to facilitate reporting structures;
- Business Sites – identifying physical locations where workers perform job functions;
- Job Profiles – identifying and creating job information that will be associated with a worker including a job code, job description, and pay rate type;
- Headcount Management – identifying and configuring one or more of the following headcount management practices (staffing models): (1) identifying individual positions to be filled; or (2) positions only limited by restrictions placed on the entire organisation;
- Worker Profile – populating detailed worker information to track across the organisation, including regulatory information, personal information, contact information, education, training, certifications and competencies;
- HR Staffing – includes hiring, terminating, transferring, promoting, and demoting of employees as well as starting/ending of contingent worker contracts;
- Manager Self Service – including demote/hire/promote/terminate and transfer employee;
- Employee Self Service – including change contact information, change business title, and change personal information;
- Onboarding – configure the Onboarding business process for new employee and contingent worker hires, campaign and announcement worklets, onboarding landing page

Payroll:

- Set-up Earning and Deduction codes;
- Set-up of general payroll rules, period schedules, run categories and pay groups;
- Configure Payroll Calculation Rules;
- Configure Payment Election Rules;

- Set-up Bank Depository and Source Bank Accounts;
- Establish Payroll Accounting to generate and review payroll accounting data;
- Configure payroll audits: compare periods & results by period;
- Create Settlement Runs.

Expenses:

- Payment Election Enrolment – define employee and contingent worker bank account information;
- Expense Item Setup – define expense items, policies, rate tables, hotel itemizations, rates, and additional attributes;
- Spend instructions - used to provide useful reminders and tips for users while creating expense reports. E.g. a link to the organisation’s expense policy on an internal website;
- Expense Credit Cards – define credit cards for corporate, personal, or mixed liability;
- Expense Reports – process reimbursement for employees, contingent workers, and applicants;
- Expense Management Dashboard – provide business intelligence for expenses, trends, and cycle times;
- Tax set up – advanced defaulting on tax applicability and tax codes to determine whether an expense is recoverable or not, and what % rate it is being taxed at;
- Employee payments – can be done through the Workday settlement engine similar to all other financial transactions which get processed and paid out.

Assumptions and Dependencies:

The Parties will agree the Functional Scope during the Plan and Architect Stages of the Workday Implementation, with appropriate consideration given to project time-line, resources and budget. As such, the proposed Functional Scope may be subject to change during these stages.

The following assumptions and dependencies were made in respect of the Functional Scope and have been relied on in compiling the estimated Charges:

HCM Core:

- Setup including tenant configuration, worker data.
- One country (England) in scope.
- Additional Jobs are out of scope.
- International Assignments are out of scope.
- A single global Onboarding process with major adjustments due customer specific requirements.
- Workday delivered organisation types with up to 5 custom organisation types (including Matrix organisations). Mapping or transformation can be performed on Locations, Cost

Centers and Company data. Manager ID data is clean and will not need transformation to create the Supervisory Organization hierarchy.

- Standard mobile functionality will be deployed, including enabling mobile domains and configuring the login process. No custom setup will be done.
- HR administration is done by a decentralized team but is managed by a centralised team.
- Up to 5 Custom Security Groups.
- Up to 5 Letter templates (e.g. generation of confirmation of job changes, ad hoc compensation changes).
- e-Signature integration is out of scope.
- Additional languages: translation of non-tenanted (customer owned configuration) data (e.g. Compensation Plan names) is out of scope.
- Foundation tenant is out of scope.
- Initial configuration of Workday Core HCM.
- A single set of global (HCM) business processes based on Workday delivered definitions with one or two step approval. Up to a total of 16 global Validations, To Do steps, Condition Rules or Notifications. Configuration of the Request Framework is out of scope.
- Organisations in scope (including related hierarchies):
 - Supervisory
 - Up to 8 companies
 - Up to 5 matrix orgs
 - Up to 5 custom orgs types with up to 100 instances of each type
 - Up to 500 cost centres
 - Up to 8 pay groups.
- Organisations out of scope:
 - Regions
 - Business units
 - Unions
 - Retiree orgs.
- Jobs and Staffing:
 - Up to 10 job family groups
 - Up to 50 job families
 - Up to 1000 job profiles
 - 1 management level hierarchy
 - Up to 25 work shifts.

Core Compensation:

- Up to 15 allowance plans (regular guaranteed cash earnings) globally.
- Salary benchmarking configuration and data is out of scope.
- No custom Compensation Basis.
- Standard set of global business processes with standard one or two step approval (Request Compensation Change, Request One Time Payment, Propose Compensation Hire, Propose Compensation Change). Up to a total of 8 global validations, To Do Steps or Condition Rules. Workday standard notifications.
- No collective labour agreements (including factor options).
- No commission plans.
- Base configuration of compensation, including a total of 1 compensation package, 1 salary plan and 1 hourly plan.
- Future payment, unit allowance and unit salary plans are not in scope.
- Merit, bonus and stock plans are out of scope.
- Compensation segment security is out of scope.
- Post termination compensation is out of scope.
- No Custom Compensation Basis for Managing by Basis Total.
- Up to 10 grades and grade profiles (defined compensation ranges) per population. Total of 10 globally.
- No grades / grade profiles that include step progression (automated pay rises to discrete compensation amounts).
- Basic KT of Workday Compensation module components to assist customer in maintaining functionality.
- Up to 15 one-time payment plans globally.
- No period salary plans (additional months of pay - e.g. 13th month) configured.
- Workday delivered reporting only.

Benefits:

- Up to 8 benefits plans. Custom eligibility based on benefit plan policies.
- Up to 10 benefit event types.
- Workday delivered reporting only.
- 2-hour remote Buyer Confirmation Session.
- Benefits credit functionality is out of scope.
- 1 enrolment event rule.

- 2 benefit groups.
- Integrations with benefit providers are out of scope unless specifically identified and estimated as part of the integrations scope.

Absence:

- Up to 17 absence plans per distinct population, implemented and unit tested by the supplier. 1 distinct population group per country (worker groups with different terms and conditions of employment relating to absence). Mixture of time off and leave types. Mixture of complexity based on a typical implementation: 20% complex plans with accruals/carryover/pro-ration/payout, 50% plans with simple balance tracking, 30% simple plans that do not track a balance.
- Review and revision following testing. This assumes minimal revision is required and the plans specified require simple changes to names, key numbers, condition lists. Excludes changes in eligibility or calculation requirements.
- Mapping of time offs to payroll system (paid/unpaid). One external system per payroll mapping. Assumes codes are provided to match specified plans.
- One holiday calendar per country with a simple location-based eligibility rule. Full day holidays only.
- Up to 10 work schedules globally, simple location-based eligibility. Work schedule patterns do not exceed 2 repeating weeks. Knowledge transfer session to understand data template. Buyer populates Workday template.
- Standard set of global business processes with standard one or two step approval (Request Absence, Request Time Off, Request Leave of Absence, Correct Absence, Correct Time Off, Correct Leave of Absence, Assign Work Schedule, Absence Calendar, Time Off Balance Transfer). Addition of standard processing steps to Hire, Termination, Change Job. Up to 8 global validations or 'to do' steps. Workday standard notifications.
- Delivered Absence reporting only.
- No questionnaires will be included in business processes.
- Review of Absence workbook in country specific sessions.
- 2-hour Buyer confirmation session + 1-hour preparation and follow up per country to review configuration. Delivered remotely.
- Basic knowledge transfer of Workday functional area to assist Buyer in maintaining functionality. Workday documentation links also provided.
- Multiple positions are out of scope

Talent:

- A single global Manage Competencies process and setup for up to 50 Competencies (including their association with Job Families, Management Levels and/or Job Profiles as required).

- A single global Development Plan process with 2 Development Plan templates and related Employee Review setup.
- A single global Disciplinary Action Plan process with 2 Disciplinary Action Plan templates and related Employee Review setup.
- Performance improvement plans are out of scope.
- A single global Performance Review process with up to 5 Performance Review templates (e.g. Goal Setting, Mid-Year and End of Year review templates with different evaluation criteria for individual contributors and managers) and related Employee Review setup.
- A standard set of global processes for up to 3 Feedback types (i.e. Unsolicited, Role Requested and Self Requested) and related Feedback setup.
- A single global Manage Goals and Cascade Goals process and related Goal setup. Organisation Goals. Up to 4 global validation conditions.
- Performance Calibration is out of scope.
- A single global standalone Assess Potential / Assess My Team's Potential process and up to 4 Potential Assessment values (Potential; Achievable Level; perceived risk of leaving the company (Retention Risk) and potential Loss Impact).
- 1 day of on-site Buyer confirmation sessions.
- A standard set of global processes for up to 8 Skills & Experience types and related setup. Up to 4 global validation conditions.
- A single global Manage Succession Plan process, Succession Plans for leadership roles and related Succession / Readiness setup.
- Talent calibration process is out of scope.
- Talent Reviews are out of scope.

Recruiting:

- Up to 10 custom notifications (e.g. 'Thank you for applying. Unfortunately, you haven't been successful on this occasion.')
- Buyer Confirmation Sessions typically take place over two days and best practice is that the Buyer SME will lead with support from the build consultant. The hours entail on-site time and planning between the lead, build consultant and client SME.
- No data migration (prospects/job requisitions/candidates).
- Up to 25 questions in recruiting applicant process.
- Up to 50 Recruiting agencies including a single recruiting agency account per agency.
- Single global offer process, 1 x Workday standard internal career site, 1 x Workday standard external career site, up to three offer letters, no contract generation, a single global approvals process for the creation of positions, job requisitions & offers.
- Workday delivered Recruiting reports only.

- Client SME or HRIS person to take ownership of recruiting custom notifications and basic recruiting configuration tables.
- Cutover strategy is such that all existing job requisitions continue to be managed under existing system as of the go-live date, new job requisitions are opened in Workday.
- Documents (e.g. Offer letter) will be delivered in a single language (if additional document translations are required this will incur additional cost and the Buyer will provide the translated text).

Reporting:

- 100 hours of custom reports will be in scope. This will include analysis of standard reports to fit Buyer needs within budget, defining custom report needs, building of in scope reports (including those necessitated by the Buyer's data purge requirements), and testing report output.
- 20 hours of additional knowledge transfer will be in scope. This will include support in functional questions as well as in reporting.

Payroll

Assumes:

- 150 earnings and deductions
- Up to 3 Pension Schemes
- Up to 10 medium complexity pay calculations
- Up to 2 bank account
- 2 parallel runs
- First of month go live
- Up to 2 PAYE Ref
- BACS processing agent in place i.e. Bottomline or ePay

Payroll Setup:

- Configure Period Schedule & Run Category
- Configure Pay Group
- Set up Company tax information (PAYE)
- Set-up Earning and Deduction codes;
- Configure Payroll Calculation Rules;
- Configure Payment Election Rules;
- Set-up Source Bank Accounts;
- Establish Payroll Accounting;

- o Configure payroll audits: compare periods & results by period;
- o Configure Payroll Gross to Net
- o Configure Auto Enrolment (Pensions)
- o Configure HMRC RTI Integrations (Incoming, FPS & EPS)
- o Configure Payroll EIBs
- o Settlement Runs
- o Configure BACS

Reports:

- o Pay Calculation Results - Deduction Register
- o Pay Calculation Results - Earning Register
- o Pay Calculation Results for Group of Workers
- o Audit - Pay Calculation Results Comparison to a Prior Period (By Worker) – Configured to client spec for variance
- o Audit - Pay Calculation Results for a Period – Configured to client spec for variance
- o Pay Calculation Results Summary
- o Payroll Accounting by Company/Period
- o Payroll Register by Period
- o UK FPS Amounts Reported To HMRC
- o UK RTI FPS Data
- o UK RTI FPS Exceptions
- o UK RTI EPS Data
- o UK RTI Submission Responses
- o Payroll Gross to Net

Payroll History – Data:

- o Load current tax year YTD - Up to 2 tests and 1 production load.

Considerations of items that are not included:

- o Reports or integrations for pension providers or any other non-Workday delivered report not list above.
- o BACS Processing agent Integration i.e. sFTP
- o External GL Integration for Payroll Accounting
- o Consultant support is estimated as remote support.
- o Volume of Data - i.e. loading more than just current tax year figures

Expenses:

- Expenses will be paid off before cutover and no data conversion of Expenses is required
- Any historic data requirements will be available from legacy systems
- No integrations with a 3rd party travel desk are required
- Only 1 country (UK) in scope
- Exchange rates loaded to allow claiming of FOREX expenses
- Utilises standard, provided reports. No budget included for extra report writing
- Assumes standard VAT complexity around expenses
- Home worker tax compliance is not in scope
- Standard BP's used
- Assume will use mobile as well as desktop for expense and receipt entry
- Create a settlement run for payment of Expenses

Part B – Integration Scope

The below assumptions and dependencies were made in respect of the Integration Scope and have been relied on in compiling the estimated Charges:

- The following integrations are in scope for discussion:
 - Active Directory (“AD”) (in)
 - Assuming there is one central AD (single AD forest I think it's called) and we don't have to serve multiple AD instances. Assuming direct connection to AD is possible, not via another system. Assuming AD system does not feed further downstream systems.
 - Assuming Studio used as technology
 - Assuming full file import, file format XML, CSV or fixed-length text.
 - Assuming importing employee login, email, possibly phone and location information.
 - Assuming AD will provide employee Workday ID for inbound messages.
 - Active Directory (out)
 - Assuming typical AD integration. No AD connector usage, EIB based. Sending information on basic employee demographics (30 fields). Assuming full file sent.
 - Workday is responsible for Employee ID generation

- AD is responsible for creating usernames and work emails, that are then sent back to Workday
- There is one AD domain that integration sends data to
- Only basic HR fields are sent, no complex mappings
- Delivery to Buyer's SFTP server
- Assuming there is one central AD (single AD forest I think it's called) and we don't have to serve multiple AD instances. Assuming direct connection to AD is possible, not via another system. Assuming AD system does not feed further downstream systems.
- Output file will be transformed to either an XML, CSV or fixed length file based on external system requirements.
- SSO (SAML)
 - Assuming single identity provider for Workday system and no complex authorization rules required
 - Assuming that authentication is done using SAML2 protocol.
- MyCSP
 - Assuming outbound only benefits connector
 - Assuming integration based on Workday benefits connector and Workday Studio
 - Assuming complex custom report build required with additional calculated fields
 - Assuming data mapping is performed by Workday integration
 - Assuming integration only handles changes, does not support deleting items from MyCSP
 - Assuming Workday benefits configuration will be aligned to MyCSP requirements
 - Assuming partial reusability of code developed by Supplier for prior Workday clients for MyCSP integration
 - Assuming following MyCSP files are supported:
 - Basic Data
 - Address
 - Service History
 - Part Time History
 - Salary History
 - Payment History
 - Control Totals
 - Short-Time Hours History – Single Records
 - Short-Time Hours History – Accumulated Records

- Scheme Contribution Rate History
- Assuming following My
 - Allowance History
 - Bonus History
 - WPS Contribution Rate History
- Navision
 - Assumes only outbound feed to Navision to populate system with Worker information. Any other feeds (customers sync, invoices sync) would have to be estimated separately.
 - Assumes medium complexity Core Connector Worker based integration
 - Assumes data transformation will be required, medium complexity
 - Assumes only data available via Core connector Worker will be on the output
 - Assumes data feed will include employee personal information, position data, new hires, terminations, job changes
 - Assumes outbound file format is XML or CSV
 - Assuming no international assignments or multiple positions are covered.
- HMRC
 - Assuming all HMRC integrations will be based on Workday-provided templates and will require minimal configuration and testing
- Civil Service Learning
 - Assumes medium complexity Core Connector Worker based integration
 - Assumes data transformation will be required, medium complexity
 - Assumes only data available via Core connector Worker will be on the output
 - Assumes data feed will include employee personal information, position data, new hires, terminations, job changes
 - Assumes outbound file format is XML or CSV
 - Assuming no international assignments or multiple positions are covered.

Part C – Data Loads

The following assumptions were made in respect of Data Loads and have been relied on in compiling the estimated Charges:

The Buyer will be responsible for preparing data in an agreed format suitable for loading in Workday. Data conversion will include the following:

- Current data records for all active employees and employees terminated in the previous 12 months will be included in the data conversion to the Workday Service. Identified Workday-supported human resources history will be selected for conversion during the Architect Stage of the project and will be loaded only into Workday’s ‘Maintain Worker History from prior system’ object for the purposes of viewing data and reporting;

- Supplier will provide a conversion template that Buyer will populate with Buyer’s extracted and transformed data. The Supplier data conversion consultant will use the completed templates to load the data into the Workday tenant.
- The Buyer will be responsible to ensuring that any input required from external parties (e.g. SSCL) is delivered within the specified format and within the required time constraints to avoid delays
- The Supplier will provide Data Gathering Workbooks that Buyer will populate with their extracted and transformed data. The Supplier Data Conversion Consultant(s) will use the completed templates to load the data into the Workday tenant. Buyer will provide all data e.g. employee, country data in one workbook. No other worker types as outlined are included in the data conversion. If any of these are deemed in scope, a separate change order will be created.
- Current data records for up to 7000 active employees will be included in the data conversion to the Workday Service
- Current data records for up to 500 contingent workers will be included in the data conversion to the Workday Service
- Up to 1000 terminated workers will be included in the data conversion to the Workday Service
- Data conversion for retirees is out of scope
- 1 Country in scope
- Loading data for Transactional History is out of scope
- Up to three years of history for Job and Compensation changes will be converted as Previous System History
- Data conversion of Custom Objects to the Workday Service to support legacy system is out of scope
- Loading of Absence Management Balances, and history for current year from previous system is in scope
- Loading of historical Talent and Performance data from previous system is in scope
- UK Payroll in scope
- Buyer have knowledge about data and Supplier isn't required to provide additional support for data mapping or extracting
- It is the responsibility of Buyer to provide clean and complete data based on the template requirements. If data discrepancies or errors are discovered, it is up to Buyer to troubleshoot and resolve. Supplier will not perform data cleansing activities
- Top of stack benefits elections for current plan year are loaded only
- Dependent data for Benefits is only stored in one system and quality is considered clean

Part D – Worker Populations

The assumed Worker Populations are as follows and have been relied upon in compiling the estimated Charges:

Country	Number of Active Employees (Approx.)	Language
United Kingdom	7000	English

Part E – Post-Deployment Support Services

The following assumptions were made in respect of Data Loads and have been relied on in compiling the estimated Charges:

The Supplier will support the following items for all Modules deployed by the Buyer during the Service Period:

- Workday Configurations
- Workday Business process and security
- Workday Integrations
- Workday Custom Reports

Collectively the Supplier Post-Deployment Support Application Management Service (AMS).

Incident Logging Procedure: Incidents should be logged by the Buyer through KIM (Kainos Incident Management). In addition to raising a KIM request, although not required, the Buyer may also contact the Supplier Service Desk on: +44 28 9057 1860.

The standard Service Hours for AMS are: Monday to Friday 0900-1700 GMT Excluding UK public holidays

The Post-Deployment Support Application Management Service provided by the Supplier comprises:

An available named Service Manager to:

- Service Management
- Manage the service initiation of AMS services
 - Manage the AMS team to deliver the AMS service;
 - Respond to requests for service within the SLA and progress appropriately;
 - Set up and on-going access to KIM (Kainos Incident Management) for the Buyer which will provide Incident history and traceability for each request
 - Monthly MI reporting including utilization of time, breakdown of services provided by functional area, status summary of open service requests,
 - Regular progress meetings (minimal monthly)
 - Quarterly onsite service reviews.

Telephone Advice and Assistance

To address Buyer enquiries in respect of the use or operation of the Supported Items during the Service Hours, within the Service Period.

- Reporting services
- The provision of status updates by Supplier to the Buyer in the form of monthly status reports detailing Incidents raised;
 - SLA metrics for all requests raised;
 - Any potential recommendations or AMS improvements;

- Quarterly status meetings with the Buyer to review the AMS.
 - Provision of temporary or permanent corrections to the Supported Items where Incidents have been escalated from 1st and 2nd Line Tier (and where approval has been provided) to implement changes that cover:
 - Test of correction or changes on the client non-Production environment; and
 - Deployment of correction or change to the Production environment;
 - Qualified personnel to provide support during the Service Hours and
 - Investigate Incidents with the Supported Items;
 - Provision of consultancy services to Buyer's 1st and 2nd Tier Support (if required);
 - Provision of estimates on the length of time to correct Incidents;
- 3rd and 4th
Tier Support
- Investigation and assessment of any Third Party Software changes and the
 - Possible impact on the Workday Service with recommended actions;
 - Augment Buyer support teams with Supplier AMS staff (if required);
 - Deliver configuration review and optimisation programmes (if required).

Additional services that can be drawn down from AMS days include:

- Pro-active monitoring of Integrations
- Testing of Workday Updates
- Tenant health check and audits
- Test consultancy
- Data loading

The Buyer will:

- promptly notify the Supplier of any incidents it becomes aware of using the AMS Incident logging procedure set out above.
- provide 1st and 2nd Tier Support, this involves:
 - performing initial investigation and assessment of Incidents (to include liaising with Buyer users to obtain all the relevant detail and error analysis information);
 - resolving straightforward issues and Incidents (for example and without limitation, data issues or simple configuration changes);
 - logging Incidents requiring more detailed investigation and providing a full description and information in the Kainos Incident Management (KIM);
 - prioritising Incidents based on the Incident classifications set out in the Order Form;
 - providing interface between 3rd and 4th Tier Support and Buyer users and providing Incident feedback and appropriate workarounds to Buyer users;
 - keeping informed of Workday Updates and supply details to Buyer users on new features;
 - facilitating testing of changes on non-Production environment;

- scheduling changes that need to be applied by Supplier to the production system (once testing has been confirmed as successful);
 - creating backup requests (Customer Centre) prior to major production changes;
 - managing Third Party Software supplier relationships and the notification of changes to the Supplier (via KIM) of any Third Party Software systems to allow Supplier to impact assess the changes on the Workday Service;
 - close Incidents;
 - support any software or equipment with which the Supported Items or Workday Service interacts;
 - liaise directly with Workday for resolution of Workday Service issues;
 - ensure Workday Update regression test activities are planned and executed in timely manner;
 - fulfil its obligations under the Call-Off Contract.
- be responsible for:
 - supplying any third party VPN software if required to remotely access the Buyer's platforms;
 - ensuring access is afforded to Supplier, or required third parties to its production and suitable non-production environments as required;
 - the appointment of a member of its staff to act as the principal point of contact between the Parties who will act as the first point of contact with the Supplier in the investigation of Incidents and other support requirements;
 - making available to Supplier free of charge all information, facilities and services reasonably required by Supplier to enable Supplier to perform the Services;
 - providing suitable office accommodation and services, including internet and telephone facilities to Supplier staff where there is a requirement for Supplier to work on-site. Failure by the Buyer to meet the Buyer Responsibilities set out in this clause may impact the charges, the provision of the Services, the timely investigation of Incidents and the SLA.

Further details on the service provision is available within the Service Definition document from G-Cloud.

Links below to this document, the Supplier's T&C's and the response to our Functional requirements:



108910173805379-t 108910173805379-s
 erms-and-condition-service-definition-do

Response redacted

Workday automated testing SaaS, Smart™ (“Smart”).

The Buyer has the option, but not the obligation, to procure Smart during the Call-Off Contract term at the charges set out in Annex 1.

Service Description

Smart is a SaaS test automation product for Workday implementations. This powerful and easy-to-use tool allows teams to test HCM, Financials, and Payroll business processes, security configurations and integrations. Smart allows the Buyer to automate the creation, execution and verification of test cases against their specific Workday configuration. Once created, the Buyer's test cases can be re-used time and again.

Features

- Covers HCM, Payroll & Financials business-process, Security configuration and Integration-testing
- Allows automated execution and verification of test cases against specific-Workday-configuration
- Test automation is pre-built and continually-maintained by the Supplier against latest-Workday-version
- Proven testing methodologies for HCM, Payroll, Security and Financials
- Scheduling of concurrent test-execution on multiple-tenants enabling high-volume of test-execution
- Reporting capability that consolidates results from multiple test runs
- Troubleshoot tests failures at-a-glance with screenshots that show failure-location/ error-message
- Secure storage location to share documents and data
- Complete toolkit to assist with the creation of test data
- API that enables integration with ALM and CI tools

Benefits

- Tests the security of the Buyer's Workday population and monitors and reports on change
- Full end-to-end testing of business-critical transactions, improving test coverage/quality
- Reduces testing effort, timescales and costs during implementation and ongoing-regression-testing
- Reduces overall testing and maintenance burden on your SMEs
- Frees-up staff time to take advantage of and adopt new Workday features
- Improves auditability of testing by producing transparent, concise audit evidence
- Reduces risk in Workday implementations and ongoing BAU changes
- Improves confidence levels of Buyer's security configuration
-

Service Details

Smart works by automating scripts that test key elements of the Buyer's Workday deployment. Our The automation that has been pre-built and is continuously maintained by the Supplier meaning that the Buyer doesn't need to write and maintain its own automation scripts.

Using Smart test automation saves time on test effort on all key areas across Workday. This includes testing business processes related to Hire, Compensation, Benefits, Absence and Time Tracking.

With Smart Financials, you can focus testing on the highest risk areas in Workday Financials, such as Journal Entry, Customer and Supplier Chain, Custom Validation Rules and Account Posting Rules testing.

Smart Payroll enables testing of Pay Components, Pay Stubs, Plans, Limits, Taxation, and Effective Dated Changes.

With Smart Security, you can test your Workday Security configuration to ensure workers have the required access to data and actions. Crucially it also checks data and actions that they shouldn't have access to.

Alongside the Smart product is a suite of implementation services delivered by our expert team of Workday certified consultants in line with our industry best -practice methodologies. All Smart implementations are tailored to suit the specific requirements and timelines of the Buyer and typically cover the following objectives:

- Kick Off

The Supplier team provision the Buyer's Smart tenant including connectivity to your Workday tenants

- Plan Stage

A series of collaborative meetings to agree an implementation plan (timelines), agree and qualify the success objectives, identify test pack requirements and establish governance procedures

- Delivery Stage

The Supplier build and deliver the Smart test packs as agreed with the Buyer during plan stage

- Knowledge Transfer & Training

On-site knowledge transfer workshop to complete handover of test packs and ensure the customer team are self-sufficient going forward

- Support

Allocation of a Success Manager and access to the Smart Support team throughout the life of the Smart subscription.

See G-Cloud Services required section above.

Schedule 2 - Call-Off Contract charges

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

Item	Estimated Cost (excluding Vat)
Implementation of Workday HCM, Payroll and Expenses	Redacted Year 1 payment (Feb to March 19) Redacted Year 2 payment (April 19 to Dec 19) Redacted
Post-Deployment Support Application Management Service (AMS) (2 years)	Redacted Year 1 payment (Dec 19 to March 20) = Redacted Year 2 payment (April 20 to Jan 21) = Redacted
Estimated Total (Years 1 & 2)	Redacted
<p>If the Buyer exercises its option to extend the Call-Off Contract in year 3, the estimated Charge for Post Development Support Application Management Service (AMS) will total Redacted.</p> <p>For the avoidance of doubt, the Buyer is under no obligation to extend the Call-Off Contract beyond the initial 24 month term.</p>	
Estimated Total (Years 1, 2 & 3)	Redacted

The value above represents the full potential value of this contract. It does however contain optional costs for additional support days.

The actual committed contract value for the initial 24-month term is **Redacted** (excluding VAT).

Further details on the SFIA rate card from the Service Offering on Cloud is attached as well as the Supplier's response to the Cost Model during the Clarification exercise.



108910173805379-p
ricing-document GC Cost Model redacted

In addition to the above, the Buyer has the option, but not the obligation, to procure Smart during the Call-Off Contract term. The Buyer shall advise the Supplier's principle contact, as set out above, should it

wish to exercise its option to avail of Smart. The parties will use the G-Cloud Variation Process to contract the Smart option.

The Smart Order Form is set out in Annex 1. Upon election of the option, this will be completed and executed as part of the Variation Process. The Order Form will stipulate the number of FSEs and the Smart module that the Buyer wishes to procure. Pricing will be calculated based on the rates set out below (also found on the Digital Marketplace):

Number of FSE (Full Service Equivalent)	Price for any 1 module	Price for any 2 modules	Price for any 3 modules	Price for all 4 modules
Up to 2,000	£24,000	£24,000	£48,240	£57,600
2001 – 4,000	£32,000	£32,000	£64,320	£76,800
4,001 – 10,000	£48,000	£48,000	£96,480	£115,200
10,001 – 20,000	£56,000	£56,000	£112,560	£134,400
20,001 – 30,000	£64,000	£64,000	£128,640	£153,600
30,001 – 40,000	£72,000	£72,000	£144,720	£172,800
40,001 – 50,000	£80,000	£80,000	£160,800	£192,000
50,001 – 60,000	£88,000	£88,000	£176,880	£211,200
60,001 – 70,000	£96,000	£96,000	£192,960	£230,400
70,001 – 80,000	£103,000	£103,000	£207,030	£247,200
80,001 – 90,000	£111,000	£111,000	£223,110	£266,400
90,001 – 100,000	£119,000	£119,000	£239,190	£285,600
100,001 – 120,000	£127,000	£127,000	£255,270	£304,800
120,001 – 140,000	£135,000	£135,000	£271,350	£324,000
140,001 – 160,000	£143,000	£143,000	£287,430	£343,200
160,001 – 180,000	£151,000	£151,000	£303,510	£362,400
180,001 – 200,000	£159,000	£159,000	£319,590	£381,600
200,000+	£167,000	£167,000	£335,670	£400,800

Part B - Terms and conditions

1. Call-Off Contract start date and length

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.2 to 5.3 (Force majeure)
- 5.6 (Continuing rights)
- 5.7 to 5.9 (Change of control)
- 5.10 (Fraud)
- 5.11 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

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

6. Business continuity and disaster recovery

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

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

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

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

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

13. Buyer data

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

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

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

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

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

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

- the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Accreditation of Information Systems at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/guidance/risk-management-collection>

- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

- 13.6 The Buyer will specify any security requirements for this project in the Order Form.
- 13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

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

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
 - Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

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

17. Guarantee

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

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

20. Notices

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

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

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
 - there will be no adverse impact on service continuity
 - there is no vendor lock-in to the Supplier's Service at exit
 - it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

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

22. Handover to replacement supplier

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

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

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

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

23. Force majeure

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

24. Liability

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

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

25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
- comply with any security requirements at the premises and not do anything to weaken the security of the premises
 - comply with Buyer requirements for the conduct of personnel
 - comply with any health and safety measures implemented by the Buyer
 - immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
- 25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

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

- 26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.
- 26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

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

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

28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- the activities they perform
 - age
 - start date
 - place of work
 - notice period
 - redundancy payment entitlement
 - salary, benefits and pension entitlements
 - employment status

- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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 (Not Used)

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

Schedule 4 - Alternative clauses (Not Used)

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

Schedule 5 – Guarantee (Not Used)

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

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).

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

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

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

Force Majeure	<p>A Force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	<p>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).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.10 together with the Framework Schedules.</p>
Fraud	<p>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.</p>
Freedom of Information Act or FOIA	<p>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.</p>
G-Cloud Services	<p>The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier</p>

	Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government guidance and the Crown Commercial Service guidance, current UK Government guidance will take precedence.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: <ul style="list-style-type: none"> ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: <ul style="list-style-type: none"> ● 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

	<ul style="list-style-type: none"> ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> ● the supplier's own limited company ● a service or a personal service company ● a partnership <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>
IPR Claim	A claim as set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.

Processing	Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: <ul style="list-style-type: none"> ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.

Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off

	Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - Processing, Personal Data and Data Subjects

Subject matter of the processing:

The processing is needed, and restricted to, the Workday HR, Payroll and Expenses functionality within the Buyer's Organisation in order to ensure that the Supplier can effectively deliver the contract to successfully implement the Buyer's Workday functionality within the Buyer's Organisation. This will involve data migration; data validation / testing; and Workday Application Management Services to provide Workday HR, Payroll, Data and Integrations support.

Duration of the processing:

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

Nature and purposes of the Processing:

On the instructions of the Controller in respect of the Controller's Workday project means any operation such as:

- collection;
- recording;
- organisation;
- structuring;
- storage;
- adaptation or alteration;
- retrieval;
- consultation;
- use;
- disclosure by transmission;
- dissemination or otherwise making available;
- alignment or combination;
- restriction;
- erasure or destruction of data (whether or not by automated means)
- employment processing;
- statutory obligation;
- recruitment and on-boarding;
- absence management;
- performance and talent management;
- Learning and Development; and
- expenses and payroll processing.

as required by the Controller.

Type of Personal Data:

The type of Personal data includes:

- name,
- address,
- date of birth,
- NI number,
- telephone number,
- pay,
- contact information (including home and work address, phone numbers, next of kin details),
- marital status,
- ethnicity,
- bank details,
- gender, disability information,
- employee identification number,
- probation period,
- visa information;
- passport information;
- military service information;
- religion information;
- education,
- language(s) and special competencies;
- certification information;
- probation period and employment duration information;
- job or position title;
- cost center work schedule/pattern (full-time or part-time, regular or temporary);
- compensation and related information (including pay type and information regarding raises and salary adjustments);
- payroll information;
- allowance, bonus, commission;
- leave of absence information;
- employment history;
- training and development information;
- award information; and
- membership information.

Categories of Data Subject:

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

Controller staff, candidates, former staff (including full time, part time, contract/temporary staff and affiliates)

Dependents / beneficiaries of Controller staff where benefits records are in scope

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:

At the written direction of the Buyer, the Supplier will delete or return Personal Data (and any copies of it) to the Buyer on termination of the Agreement, unless the Supplier is required by Law to retain the Personal Data in accordance with the relevant provisions of Terms and Conditions.

Schedule 8 – Additional Buyers Terms and Conditions

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

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

1. Departmental Security Standards

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

	website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
“Cyber Essentials” “Cyber Essentials Plus”	<p>Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: https://www.iasme.co.uk/apply-for-self-assessment/</p>
“Data” “Data Controller” “Data Processor” “Personal Data” “Sensitive Personal Data” “Data Subject”, “Process” and “Processing”	shall have the meanings given to those terms by the Data Protection Act 2018
"Department's Data" “Department's Information”	<p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including:</p> <p>(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:</p> <p style="padding-left: 40px;">(i) supplied to the Contractor by or on behalf of the Department; or</p> <p style="padding-left: 40px;">(ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or</p> <p>(b) any Personal Data for which the Department is the Data Controller;</p>
“DfE” “Department”	means the Department for Education
“Departmental Security Standards”	means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.

“Digital Marketplace / GCloud”	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.
“FIPS 140-2”	this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled ‘Security Requirements for Cryptographic Modules’. This document is the de facto security standard used for the accreditation of cryptographic modules.
“Good Industry Practice” “Industry Good Practice”	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“Good Industry Standard” “Industry Good Standard”	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“GSC” “GSCP”	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
“HMG”	means Her Majesty’s Government
“ICT”	means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise

<p>“IT Health Check (ITHC)” “Penetration Testing”</p>	<p>the confidentiality, integrity or availability of information held on that IT system.</p>
<p>“Need-to-Know”</p>	<p>the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.</p>
<p>“NCSC”</p>	<p>The National Cyber Security Centre (NCSC) formerly CESG is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk</p>
<p>“OFFICIAL” “OFFICIAL-SENSITIVE”</p>	<p>the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services.</p> <p>the ‘OFFICIAL–SENSITIVE’ caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.</p>
<p>“Secure Sanitisation”</p>	<p>Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable.</p> <p>Secure sanitisation was previously covered by “Information Assurance Standard No. 5 - Secure Sanitisation” (“IS5”) issued by the former CESG. Guidance can now be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</p> <p>The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction</p>
<p>“Security and Information Risk Advisor” “CCP SIRA”</p>	<p>the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme.</p> <p>See also:</p>

"SIRA"	https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"SPF" "HMG Security Policy Framework"	<p>This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.</p> <p>https://www.gov.uk/government/publications/security-policy-framework</p>
"Tailored Assurance" [formerly called "CTAS", or, "CESG Tailored Assurance"]	<p>is an 'information assurance scheme' which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks.</p> <p>https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology</p>

The Supplier shall comply with Buyer's Security Standards for Contractors which include but are not constrained to the following clauses.

- 1.1. Where the Supplier will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Buyer, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - [Action Note 09/14](#) 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme”. The certification scope must be relevant to the services supplied to, or on behalf of, the Buyer.
- 1.2 The Supplier shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
- 1.3 The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer's Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).
- 1.4 Buyer's Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Buyer's Data then the Supplier and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.
- 1.5 The Supplier shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas
- 1.6 The Supplier shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Buyer's Data.
- 1.7 The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating

systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.

- 1.8 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which has been certified to FIPS 140-2 standard or a similar method approved by the Buyer prior to being used for the transfer of any Buyer's Data.
- 1.9 Storage of Buyer's Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.11 and 1.12 below.
- 1.10 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Buyer's Data to deliver and support the service, shall be under the control and configuration management of the Supplier or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Buyer.
- 1.11 All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Buyer's Data to deliver and support the service, shall be under the control and configuration management of the Supplier or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Buyer.
- 1.12 Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.
- 1.13 When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.
- 1.14 At the end of the contract or in the event of equipment failure or obsolescence, all Buyer information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Supplier's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Supplier or sub-contractor shall protect the Buyer's

information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

- 1.15 Access by Supplier or sub-contractor staff to Buyer's Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Supplier's or sub-contractor staff must complete this process before access to Buyer Data is permitted.
- 1.16 All Supplier or sub-contractor employees who handle Buyer Data must have annual awareness training in protecting information.
- 1.17 The Supplier shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the Supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 1.18 Any suspected or actual breach of the confidentiality, integrity or availability of Buyer Data being handled in the course of providing this service, or any non-compliance with these Buyer Security Standards for Suppliers, or other Security Standards pertaining to the solution, shall be investigated immediately and escalated to the Buyer by a method agreed by both parties.
- 1.19 The Supplier shall ensure that any IT systems and hosting environments that are used to handle, store or process Buyer Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Buyer and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
- 1.20 The Supplier or sub-contractors providing the service will provide the Buyer with full details of any storage of Buyer Data outside of the UK or any future intention to host Buyer Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Supplier or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Buyer.
- 1.21 The Buyer reserves the right to audit the Supplier or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Supplier's, and any sub-contractors, compliance with the clauses contained in this Section.

- 1.22 The Supplier shall contractually enforce all these Buyer Security Standards for Suppliers onto any third-party suppliers, sub-contractors or partners who could potentially access Buyer Data in the course of providing this service.
- 1.23 The Supplier and sub-contractors shall undergo appropriate security assurance activities as determined by the Buyer. Supplier and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Supplier's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA)

Annex 1 - SMART ORDER FORM

(subject to Buyer electing the option to purchase Smart)

Buyer Details	
Buyer	The Secretary of State for Education (
Registered Office Address	Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
Customer Contact, Number & Email	Redacted
Invoice Contact, Number & Email	APinvoices-DFE-U@sscl.gse.gov.uk
Hosting Platform Location	EEA
Supplier Details	
Supplier	Kainos WorkSmart Limited
Registered Office Address	Kainos House, 4-6 Upper Crescent, Belfast, BT7 1NT
Kainos Contact, Number & Email	Redacted
Kimble Code	Redacted
Subscription Term	
Effective Date (start date)	30 days from receipt of notice from Buyer's notice of election to buy Smart.
End Date	As set out in Buyer's notice of election to buy Smart.

Modules	
Smart HCM Business Process & Integrations Module	<input type="checkbox"/>
Smart Financials Business Process & Integrations Module	<input type="checkbox"/>
Smart Security Module	<input type="checkbox"/>
Smart Payroll Module	<input type="checkbox"/>

Charging Bands		
Staff Number	Subscription Service Charge (annual)	Select
2001 – 4,000	£[x]	<input type="checkbox"/>

4,001 – 10,000	£[x]	<input type="checkbox"/>
10,001 – 20,000	£[x]	<input type="checkbox"/>