Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form

Platform service ID number	496633533699259

Call-Off Contract reference	Ecm_10803
Call-Off Contract title	Second Hyperscale Cloud Services
Call-Off Contract description	Provision of cloud services (Azure)
Start date	1st April 2023
Expiry date	31st March 2026
Call-Off Contract value	£21,340,181
Charging method	Invoiced Monthly in arrears
Purchase order number	TBC

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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 Services 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	[Redacted] Department for Work and Pensions Commercial Directorate Digital Blue Zone, Second Floor, East Wing Peel Park, Brunel Way Blackpool FY4 5ES
To the Supplier	Computacenter (UK) Ltd Hatfield Business Park Hatfield Avenue Hatfield Hertfordshire AL10 9TW United Kingdom Company number: 01584718
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: [Redacted]
Name: [Redacted]
Email: [Redacted]
[Redacted]

For the Supplier:
Title: [Redacted]
Name: [Redacted]
Email: [Redacted] Phone: [Redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **1st April 2023** and is valid for **36 Months**
Ending (termination)	The notice period for the Supplier needed for Ending the CallOff Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause. (as per clause 18.1) provided that the Buyer indemnifies the Supplier in respect of any sunk costs with the vendor for the remainder of the term.
Extension period	This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 4 weeks written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below, and also subject to agreement on any pricing revision for the extension. Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

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: 1 Lot 1: Cloud hosting
Services **G-Cloud Services required**	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: 1. Provision of Management Information on a monthly, quarterly, and annual basis; 2. Provision of an Account Manager and Account Management activities; 3. Provision of any Microsoft Service Management activities including adherence to all Microsoft Azure Service Levels Agreements; 4. Provision of Invoices on a monthly basis detailing all consumption for all Products used by the Customer in the Microsoft Azure Environment; 5. Provision of Training and Consultancy for all Microsoft products and services through Microsoft's provision of the Azure Tech Skills for business programme supported by the Supplier's in house expertise to advise the Customer on best build and use of Microsoft Azure Environment Products, using industry best practice to advise accordingly; 6. Identification and delivery of continuous improvement opportunities; and 7. Industry updates on Microsoft and public cloud market trends
Additional Services	Not applicable
Location	The Services will be delivered to DWP 2 St. Peters Square, Manchester, M2 3AA
Quality Standards	The quality standards required for this Call-Off Contract are standard as provided under the Microsoft Azure licensing terms.

Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are included in Supplier's Service Description documents and available on the Digital Marketplace.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are those provided by Microsoft in respect of this Azure product and those outlined in Schedule 2

Onboarding	deliver 1. boarding plan for this Call-Off Contract is based on the y of an. Agreement by both parties of the Governance and reporting content and approach within 30 days of contract start date in line with schedule 1 and 2. 2. Confirmation of the Buyer dependencies (attendance at meetings etc..) within 30 days of contract start date 3. Supplier to present an initial Continuous Improvement plan to be presented after 90 days of contract signature for review and acceptance by Buyer.
Offboarding	1. Provision of Final Invoice and Data Set 2. Inform Microsoft of termination of contract
Collaboration agreement	Not Applicable
Limit on Parties' liability	The annual total liability of the Supplier for all Defaults will not exceed the greater of **125%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).

Insurance	The Supplier insurance(s) required will be: a) a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract] b) 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) c) employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Buyer's responsibilities	The Buyer is responsible for complying with the Microsoft Azure solution terms of use.
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 monthly in arrears.
Invoice details	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.

Who and where to send invoices to	Invoices will be sent to [Redacted] Paper invoices should be sent to; SSCL, PO Box 406, Phoenix House, Celtic Springs, Newport NP10 8FZ A copy should also be emailed to the Principal Contact. [Redacted]
Invoice information required	All invoices must include • PO number, Project reference and Buyer's reference details. • Supporting data per SKU. • VAT number.
	• Document where and when specific service credits are applied and what they relate in relation to deductions from invoicing in next payment period Invoices should be presented to the DWP within 10 days of previous month end. The Buyer will pay the Supplier within thirty (30) calendar days of receipt of a valid invoice, submitted in accordance with this paragraph, the payment profile set out above and the provisions of this Call-Off Contract. Any invoices submitted by the Supplier that do not have an associated PO number(s) and accurate quantities, product details and associated costs shall be considered invalid by the DWP and shall be rejected accordingly.
Invoice frequency	Invoices will be sent to the Buyer Monthly.

Call-Off Contract value	The total value of this Call-Off Contract is £21,340,181.
Call-Off Contract charges	The breakdown of the Charges will be presented to the Buyer by the Supplier monthly in line with consumption of the Microsoft Azure service.

Additional Buyer terms

Performance of the Service

This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:

The Microsoft Azure Virtual Machine Service levels can be found at: https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-forOnline-Services?lang=1

The Service Levels will be those as set out by Microsoft and any updates to the Microsoft Service Levels will apply to this contract.

The service levels relating to the Microsoft Azure virtual machine service are:
Service Credit:
The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines deployed across two or more Availability Zones in the same region:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%
< 95%	100%

Service Credit:
The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines in an Availability Set or same Dedicated Host Group. This SLA does not apply to Availability Sets leveraging Azure shared disks:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%
< 95%	100%

Service Credit:
The following Service Levels and Service Credits are applicable to Customer's use of Single-Instance Virtual Machines by Disk type. For any Single Instance Virtual Machine

using multiple disk types, the lowest SLA of all the disks on the Virtual Machine will apply:

Uptime Percentage (Premium and Ultra SSD)	Uptime Percentage (Standard SSD Managed Disk)	Uptime Percentage (Standard HDD Managed Disk)	Service Credit
< 99.9%	<99.5%	<95%	10%
< 99%	<95%	<92%	25%
< 95%	<90%	<90%	100%

The following KPIs relate to the provision of the LSP service

KPI	Title	Requirement	Measure	Data Source
R1	Reporting Timelines	Final Reports to be provided by the second Monday each month to include: • Total Monthly Usage • Forecast Spend against Minimum Commitment • Actual Burn Down detailing Marketplace and Azure Spend • Software Marketplace Spend • Spend by Tagged instances • Spend on un-tagged instances • Service Credits • Consumption charges by business area and Product • Trend Analysis of Microsoft Azure usage • MS Azure Updates (Global) • KPI and SLA Information • Outage data including Incidents and associated service credits	100% of Reports to be delivered to the requires content and quality by 15th of each month	MI to be provided by 5pm the next business day after receiving finalised MI from Microsoft from the previous month. Report Template attached Report to be provided by 2nd Monday of the Month

	R2	Invoicing	Provide an accurate invoicing in line with usage report and to include DWP invoice amount, VAT Amount, usage, service credits.	100% of invoices provided containing required information as detailed in Invoice Template	Invoices provided in line with Usage report (above) sent monthly 1 working day after receipt from Microsoft. Invoice Template attached
	MI1	Monthly Service Review	Computacenter will attend a Monthly Service Review in person to present and discuss the MI report. Attendees will include Computacenter Account Manager, Computacenter Solution Specialist and Computacenter Azure SME. Value added information provided by the supplier will include: • Overview of previous months usage and billing • Highlight potential areas for saving • Highlight anomalous spend or usage • Opportunities to better utilise reserved and Spot instances • Impact of new provisioning on committed and forecast EA Spend • Advice on right-sizing potential workloads • Aid in the benchmarking against CIS and updating with latest versions of CIS as appropriate • Reserved Instance change/new/removal recommendations • New consumption requests raised by the DWP and fulfilled by the Supplier within the reporting period, including provision of new cloud environments orders that have not yet been invoiced • Identification of Risks/Issues raised and closed off during the accounting period, with progress status on open risks and issues. • Programme of Work Slide Deck Presentation (MS) • Review action points	Computacenter to attend100 % of monthly calls with required attendees and provide information listed by 15th of each month	Monthly Meeting minutes listing attendees - To be held 3rd Monday of the Month
	MI2	Microsoft Partner Funding	Computacenter will present opportunities to leverage Microsoft Azure Partner funding programmes to deliver services to DWP. • Prioritised List of Opportunities • Forecast Value • Actions required to deliver saving • Current progress • Dependencies • Current Status	Opportunities List provided at quarterly meetings 100% of the time	Quarterly Service Review.

Guarantee	Not Applicable

CI 1	Continuous Improvement (CI)	Submit a continuous improvement plan 90 days after the commencement of the contract and every 12 months thereafter to include: • Prioritised List of Opportunities • Point of Contact (DWP/ CC) • Forecast Value • Actions required to deliver saving • Current progress • DWP Dependencies • Current Status	Initial Plan Delivered within 90 days of contract signature Updated Plan issued 12 Months from Initial Plan Delivered	CI Report
CI 2	CI/ innovation Delivery	Supplier takes measurable against each CI initiative outlined and Monthly report detailing; • Prioritised List of Opportunities • Point of Contact (DWP/ CC) • Forecast Value • Actions required to deliver saving • Current progress • DWP Dependencies • Current Status • Risks, Action, Issues and Decisions required	100% of actions in Computacenter Plan not dependent on DWP completed	Actions Reported Monthly and reviewed in the Quarterly Service Review
SV 1	Social Value – Environmental	Carbon Emissions – related to DWP https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1054374/PPN-0621-Taking-accountof-Carbon-Reduction-Plans-Jan22__1_.pdf"	100% DWP specific Carbon Emissions reported annually	Microsoft Provided Report
SV 2	Social Value	Computacenter Carbon Emissions https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1054374/PPN-0621-Taking-accountof-Carbon-Reduction-Plans-Jan22__1_.pdf"	100% Reported Annually	Scope 1 and 2 Carbon Emissions of Computacenter Group, reported yearly.

Warranties, representations	Not applicable

Supplemental requirements in addition to the Call-Off terms	1) The Supplier's terms and conditions as submitted in its G Cloud RM1557.13 tender response shall apply and shall prevail in the event of conflict with the Call-Off terms. 2) The following clause regarding title to third party software shall apply in precedence to any Call-Off Term: a) Title in respect of software shall not transfer and shall remain at all times with the relevant licensor. 3) The following clause regarding third party software shall apply in precedence to any Call-Off Term: a) Where in the course of performing the Services, Supplier procures the grant to Buyer of a licence to use any Third-Party Software, Buyer's licence to use such Third-Party Software shall be governed by the terms imposed by the applicable third-party licensor and shall unless otherwise agreed terminate automatically where Buyer ceases to receive the related Services. 4) The following clause regarding third party services shall apply in precedence to any Call Off Term: a) Third party services (if any) shall be supplied subject to the applicable third party's standard service terms. 5) Within the scope of the Call-Off Contract, the Supplier will: a) Comply with Baseline Personnel Security Standard / Government Staff Vetting Procedures in respect of all persons who are employed or engaged by the Supplier in provision of this Call-Off Contract prior to each individual beginning work with the Buyer. This is not a security check as such but a package of pre-employment checks covering identity, employment history, nationality/immigration status and criminal records designed to provide a level of assurance. The Supplier will show evidence of these security clearances should the Buyer need sight of such evidence at any time. A Guide for DWP Suppliers' had been prepared and attached below.  BPSS 6) Protection on Information

	a) The Contractor and any of its Sub-contractors, shall not access, process, host or transfer Authority Data outside the United Kingdom without the prior

	written consent of the Authority, and where the Authority gives consent, the Contractor shall comply with any reasonable instructions notified to it by the Authority in relation to the Authority Data in question. The provisions set out in this paragraph shall apply to Landed Resources. 7) Where the Authority has given its prior written consent to the Contractor to access, process, host, or transfer Authority Data from premises outside the United Kingdom: - a) the Contractor must notify the Authority (in so far as they are not prohibited by Law) where any Regulatory Bodies seek to gain or has gained access to such Authority Data; b) the Contractor shall take all necessary steps in order to prevent any access to, or disclosure of, any Authority Data to any Regulatory Bodies outside the United Kingdom unless required by Law without any applicable exception or exemption. 8) As may be required by the Buyer from time to time, the Supplier shall provide copies of its appropriate policies to cover the following: a) Sustainability Policy b) Diversity and Equality c) Modern Slavery d) Appendix 1 details the minimum-security requirements.
Alternative clauses	Not Applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not Applicable

Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used.
Intellectual Property	Not Applicable
Social Value	Not Applicable

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 (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13

2.2 The Buyer provided an Order Form for Services to the Supplier.

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

G-Cloud 13 Customer Benefit Record .

Signed	Supplier	Buyer
Name	[Redacted]	[Redacted]
Title	[Redacted]	[Redacted]
Signature	[Redacted]	[Redacted]
Date	29 March 2023 | 11:52 BST	29 March 2023 | 13:25 BST

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 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Parties may extend this Call-Off Contract, by prior written agreement, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties agree that no exit plan is required in respect of this transaction.

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:

1. 2.3 (Warranties and representations)
2. 4.1 to 4.6 (Liability)
3. 4.10 to 4.11 (IR35)
4. 10 (Force majeure)
5. 5.3 (Continuing rights)
6. 5.4 to 5.6 (Change of control)
7. 5.7 (Fraud)
8. 5.8 (Notice of fraud)
9. 7 (Transparency and Audit)
10. 8.3 (Order of precedence)
11. 11 (Relationship)
12. 14 (Entire agreement)
13. 15 (Law and jurisdiction)
14. 16 (Legislative change)
15. 17 (Bribery and corruption)
16. 18 (Freedom of Information Act)
17. 19 (Promoting tax compliance)
18. 20 (Official Secrets Act)
19. 21 (Transfer and subcontracting)
20. 23 (Complaints handling and resolution)
21. 24 (Conflicts of interest and ethical walls)
22. 25 (Publicity and branding)

23 26 (Equality and diversity)

24 28 (Data protection)

25 31 (Severability)

26 32 and 33 (Managing disputes and Mediation)

27 34 (Confidentiality)

28 35 (Waiver and cumulative remedies)

29 36 (Corporate Social Responsibility)

30 paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

i. a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract' ii. a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer' iii. a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

a. The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

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

c. 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:

4.1.1 be appropriately experienced, qualified, and trained to supply the Services

4.1.2 apply all due skill, care, and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 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 as per clause 18.5 hereunder 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 14digit 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:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their 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 GCloud 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 portion of the 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 CallOff 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:

9.2.1 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

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 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

9.2.4 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:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 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:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 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:

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 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 incorporated Framework Agreement clause 34. 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 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates, and licensors from and against any third-party claim:

i) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law; ii) alleging that the Buyer Data violates, infringes, or misappropriates any rights of a third party;

iii) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent

such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer 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:

i. rights granted to the Buyer under this Call-Off Contract

ii. Supplier's performance of the Services iii. use by the

Buyer of the Services

11.7 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:

i. modify the relevant part of the Services without reducing its functionality or performance

ii. 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

iii. buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

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

11.9 If the Supplier does not comply with this clause 11, 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:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 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

12.1.3 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:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 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 GCloud Services.

13. Buyer data

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

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

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

13.4 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 policies and all Buyer requirements in the Order Form.

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policyframework and the Government Security Classification policy: https:/www.gov.uk/government/publications/governmentsecurityclassifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adoptrisk-managementapproach and Protection of Sensitive Information and Assets: https://www.cpni.gov.uk/protectionsensitive-information-and-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-managementcollection

13.6.4 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: https://www.gov.uk/government/publications/technologycode-ofpractice/technology -code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-securityprinciples

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 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.

13.9 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.

13.10 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 at:

https://www.gov.uk/government/publications/technology-code-ofpractice/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 all reasonable endeavours, 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:

16.4.1 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

16.4.2 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 the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's 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:

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:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 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:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover 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:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

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

18.5.1 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

18.5.2 an Insolvency Event of the other Party happens

18.5.3 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 CallOff 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 CallOff 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:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 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); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 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:

(I) return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

(II) return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

(III) 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

(IV) 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

(V) work with the Buyer on any ongoing work

(VI) return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

(VII) 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.

(VIII) 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'.

(I) Manner of delivery: email Deemed time of delivery: 9am on the first Working Day after sending

(II) Proof of service: Sent in an emailed letter in PDF format to the correct email address without any 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 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 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 take the Term beyond 36 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:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 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:

21.8.1 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

21.8.2 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

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 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:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power, or control

22.1.2 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 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

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:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 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:

29.2.1 the activities they perform

29.2.2 age

29.2.3 start date

29.2.4 place of work

29.2.5 notice period

29.2.6 redundancy payment entitlement

29.2.7 salary, benefits, and pension entitlements

29.2.8 employment status

29.2.9 identity of employer

29.2.10 working arrangements

2.11 outstanding liabilities

29.2.12 sickness absence

29.2.13 copies of all relevant employment contracts and related documents

29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

(I) 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.

(II) 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.

(III) 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.

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

(V) its failure to comply with the provisions of this clause

(VI) 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

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

(VIII) 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:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 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 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

1. Definitions

For the terms used herein the following definitions apply:

"**Account Manager**" means the person responsible within the Supplier organisation for providing Supplier requirements to the Customer.

"**Azure Portal"** means The Azure portal is a web-based, unified console that provides an alternative to command-line tools. With the Azure portal, the Customer can manage their Azure subscription using a graphical user interface.

"**Business Application**" means the Customers' applications which run in the Microsoft Azure Environment.

"**Cloud Provider**" means Microsoft Azure

"**Contract Manager**" means the Customers nominated person who will manage the Contract on a day-to-day basis

"**Contract Start Date**" means Call Off Commencement Date.

"**Customer**" means DWP

"**Customer Data**" means all data, including all text, sound, software, image or video files that are provided to the Supplier or Microsoft by, or on behalf of, Customer and its Affiliates through use of the Online Services.

"**Exit and Migration Tasks**" means activities to be carried out during any exit out of or migration away from the Microsoft Azure Environment to other hosting environment(s)

"**Exit Management Strategy and Plan**" means the Customers strategy and plan for exiting out of or migration away from Microsoft Azure Environment.

"**Governance Model**" means the interface and escalation model between the Customer and the Supplier

"**HCS Cloud Product Managers**" means the internal Customers nominated person(s) who will manage the Contract from a technical/service delivery perspective on a day to day basis.

"**Management Information**" means all information gathered by the Supplier from either it's own in house systems and services or via Microsoft systems and services in order to meet the requirements of the Customer as defined in Management Information Requirements below.

"**Microsoft Azure Environment**" means the Customers Online Services hosted environment used by the Customer and supported by the Supplier.

"Microsoft Azure Service Level Agreement" means the document specifying the minimum service level for the Online Services. The current Service Level Agreement is available at http://www.microsoft.com/licensing/contracts or a successor site.

"**Online Services**" means the Microsoft-hosted services identified as Online Services in the Product List.

"**Produc**t" means all products identified on the Product List, such as all software, Online Services and other web-based services, including pre-release or beta versions.

“**Professional Services**” means all support, consulting and other services or advice, including any resulting deliverables provided to Customer by the Supplier or Microsoft. Professional Services do not include Online Services.

“**Reserved Instance**” means hosting instances for a specified term (typically 12 months), in return for a relevant discount on the price, where it is known that they will be used on a longterm basis rather than spun up and spun down on a demand basis

“**SCE**” means the Microsoft Server and Cloud Enrolment contract between the Customer and the Supplier.

“**Service**” means all of the services delivered by the Supplier to the Customer including Online Services, Products and Professional Services.

“**Service Review Meeting**” means meetings between the Customer HCS Cloud Product Managers/Contract Manager/Supplier Relationship Manager, and the Supplier as defined in the Governance Model.

“**Subcontract**” means any contract the Supplier enters into with another third party to provide any of the Services or Products which the Supplier is contracted to provide to the Customer.

“**Supplier**” means Computacenter.

“**Supplemental Agreement**” means any agreement that incorporates the Microsoft Business and Services Agreement, or Microsoft Business Agreement signed by Customer and Microsoft

“**Supplier Relationship Manager**” means the person nominated by the Customer to perform supplier relationship activities in accordance with the Customers supplier relationship governance processes.

“**Training and Consultancy**” means the Supplier’s in house experts providing training and advice to the Customer on best practice use and deployment of Microsoft Azure Environment Products.

“**Working Days**” means normal UK business days excluding bank holidays or other public holidays declared during the life of the contract.

2. Summary of Requirements Services

2.1 In summary the requirements that the Supplier shall provide to the Customer include:

2.1.1 Provision of Management Information on a monthly, quarterly, and annual basis as defined below;

2.1.2 Provision of an Account Manager and Account Management activities as defined below;

2.1.3 Provision of any Microsoft Service Management activities including adherence to all Microsoft Azure Service Levels Agreements;

2.1.4 Provision of Invoices on a monthly basis detailing all consumption for all Products used by the Customer in the Microsoft Azure Environment;

2.1.5 Provision of Training and Consultancy for all Microsoft products and services through Microsoft's provision of the Azure Tech Skills for business programme supported by the Supplier's in house expertise to advise the Customer on best build and use of Microsoft Azure Environment Products, using industry best practice to advise accordingly;

2.1.6 Identification and delivery of continuous improvement opportunities; and

2.1.7 Industry updates on Microsoft and public cloud market trends

3. Management Information (MI) Requirements

3.1 Within the first thirty (30 Working Days of the Contract Start Date the Supplier shall work with the Customer to develop further and define a Management Information (MI) pack at the appropriate level of detail. The content detailed below at (Para 3.3) is the minimum viable product to be provided to allow the Customer to control and optimise its Microsoft Azure Environment hosting consumption including, but not limited to, all Product usage.

3.2 The Supplier shall provide such MI on a monthly, quarterly, and annual basis according to the Service Levels below. In addition, the Supplier shall provide, on an Ad Hoc basis, any other reports as requested by the Customer from time to time during the life of the contract.

3.3 This MI shall include detailed breakdown of all Products and Online services consumed by the Customer and at the minimum shall include, but not limited to, the following items, subject to the Customer purchasing the appropriate Microsoft support arrangements and/or Cloud Health:

3.3.1 Burn down data on committed spend;

3.3.2 Known Cloud Provider change windows (subject to the customer having the relevant Microsoft Support arrangements);

3.3.3 Outage data including Incidents subject to the customer having the relevant Microsoft Support arrangements);

3.3.4 Risks/issues raised and closed off during the reporting period, with progress status on open risks and issues. (subject to the customer having the relevant Microsoft Support arrangements);

3.3.5 Summarised SLA performance in accordance with the Microsoft Azure Service Level Agreements for all Products used in the Customers Microsoft Azure Environment (subject to the customer having the relevant Microsoft Support arrangements);

3.3.6 Upon Request Digital Market Place Software Licence terms;

3.3.7 Consumption data by Product line;

3.3.8 Summarised consumption by Product type (compute/Storage/software);

3.3.9 Business area consumption data by Product type (Compute/Storage/Software);

3.3.10 Consumption data by Business Application or service e.g., Tell Us Once (TUO);

3.3.11 Charging data by product line;

3.3.12 Consumption charges by product type;

3.3.13 Consumption charges by business area;

3.3.14 Charging data by Business Application or service e.g., TUO;

3.3.15 Optimisation recommendations/identification of dormant accounts (+1 month of inactivity) including re-forecasting recommendations;

3.3.16 Reserved Instance change/new/removal recommendations;

3.3.17 New consumption requests raised by the Customer and fulfilled by the Supplier within the reporting period, including provision of new cloud environments orders that have not yet been invoiced; and

3.3.18 Reports on rightsizing, utilisation, daily costs etc.

3.4 MI reporting shall be made available within the Azure Portal in real time and also included in MI packs to support review meetings. The MI pack shall be made available by the Supplier within five (5) Working Days of the end of the previous calendar month.

4. Account Management

4.1 The Supplier shall provide a nominated Account Manager who shall act as a Single Point of Contact (SPOC) for all communication relating to the Contract and for the provision of on-demand advice to the Customers nominated Contract Manager and HCS Cloud Product Manager(s).

4.2 The Supplier and the Customer shall define, within the first thirty (30) Working Days from the Contract Start Date, the appropriate Customer and Supplier Governance Model (reference Schedule 2 – Service Levels and Service Management Governance Table 6)

4.3 The Supplier shall ensure that cooperation and coordination is maintained between the Customer the Supplier and the Cloud Provider during the delivery of contracted services with the overall objective of collaboration and value add.

4.4 The Supplier shall adhere to the following principles set out below:

4.4..1 To achieve the optimal Service delivery on the basis of cooperation in partnership

4.4..2 Active maintenance of the Governance Model by both the Customer and the Supplier

4.4..3 Common usage of Service & interface processes across the Customer and the Supplier.

4.4..4 Well-defined communication channels between all identified business areas of the Customer and the Supplier

4.5 In addition, the Supplier shall provide the following account management activities:

4.4..5 The Supplier must integrate and influence the inclusion and active participation of the Cloud Provider into the overall Governance Model between the Supplier and the Customer.

4.4..6 The Supplier needs to provide advisory support to Customer in managing all aspects of the Cloud Providers performance:

- Optimise commercial performance/leverage
- Service performance
- Financial performance (optimised spend)

4.4..7 The Supplier must support the Customer in reporting the financial performance against an agreed baseline as part of the ongoing operational performance and technical delivery governance process. This is to allow the Customer and the Supplier to monitor the value being delivered by the commercial incentive offered by the Supplier and the Cloud Provider.

4.6 The nominated Account Manager must work with the Customers Supplier Relationship Manager and adhere to the Customers supplier relationship management framework

4.7 The nominated Account Manager shall have dedicated authority to make decisions relating to the Contract including management and administration activities, and the authority to sign-off/authorise contract changes.

4.8 The nominated Account Manager shall keep the Customer continuously updated on changes / upgrades to existing cloud products and keep the Customer informed of any market and product developments that might be of benefit to the Customer.

4.9 The nominated Account Manager shall notify the Customer of any changes in the Azure Portal functionality (Supplier shall specify the number of days in advance that this can be given) and shall provide a walkthrough of the changes at a scheduled session. This provision is limited to and subject to the Customer purchasing the appropriate Microsoft support arrangements.

4.10 The nominated Account Manager shall work with the Customer to

- review and help implement Microsoft Azure Environment cloud provision and consumption controls;
- support future forecasting;
- Subject to the Customer purchase of Cloud Health, identify spend optimisation opportunities; and
- identify usage efficiencies that could be implemented.

4.11 The nominated Account Manager shall be responsible and accountable for the provision of monthly Management Information (MI) and cloud consumption reporting data as defined above.

4.12 The nominated Account Manager shall attend scheduled Service Review Meetings and any ad-hoc meetings requested by the Customer.

4.13 In the event that the nominated Account Manager is removed from the Customer account, the Supplier shall provide the new incoming Account Manager with a minimum handover of twenty (20) Working Days. Such handover should be provided by the out-going Account Manager.

4.14 The Supplier will provide and maintain a clear Customer escalation process and contact details in accordance with the Governance Model which shall be reviewed, as a minimum, at quarterly Customer service meetings.

4.15 The nominated Account Manager shall support the Customer during any renewal process with the Cloud Provider bringing market knowledge and industry best practice to such discussions.

4.16 A Quarterly Account Planning Meeting must be held every three (3) months. The Quarterly Account Planning Meeting should be used to discuss any proposed updates to any plans, opportunities, review upcoming demand etc.

4.17 An annual review of performance and planning for the next 12 months including forward look on Continuous Improvement plan (identifying opportunities for efficiency over the next 12 months)

4.17 The nominated Account Manager must work with Customer to facilitate and advise on any Exit or Migration Tasks, including off boarding, should the need arise and in accordance with the Customers Exit Management Strategy and Plan.

5. Service Management

5.1. The Customer and the Supplier shall hold monthly, quarterly and annual Service Review Meetings in accordance with the Governance Model.

5.2 The monthly Service Review Meeting shall be held within ten (10) Working Days of the provision of the management information pack for the previous month (reference Schedule 2 – Service Levels and Service Management Governance Table 6).

5.3 In this meeting all Microsoft Azure Service levels as defined within shall be discussed and must include as a minimum, subject to the Customer purchasing Microsoft support arrangements, but not restricted to, the following:

- availability of the cloud services (Subject to the Customer purchase of Microsoft support arrangements)
- Closure of incidents (Subject to the Customer purchase Microsoft support arrangements)
- Provision of invoices on time
- Provision of MI

5.4 Any issues that cannot be resolved in the Service Review Meeting shall be escalated in accordance with the Governance Model (reference Schedule 2 – Service Levels and Service Management Governance Table 6).

5.5 The Supplier shall provide any reasonable ad hoc reports the Customer may specify and request within mutually agreed number of Working Days from the receipt of such requests.

5.6 The quarterly Service Review Meetings shall be held within fifteen (15) working days from the end of the quarter and shall include, subject to the Customer purchase of Microsoft support arrangements:

5.6.1 a summary of the previous quarter's performance against SLA's

5.6.2 a review of all issues and risks and any outages

5.6.3 a review of growth/decline which has occurred in the previous quarter; and

5.6.4 a review of the forthcoming implementations/growth in the next quarter.

5.7 The Annual service review meeting shall be held within 20 days of the end of the previous contract year and shall include, subject to the Customer purchase of Microsoft support arrangements:

5.7.1 a summary of the previous year's performance against SLA's,

5.7.2 a financial summary of the annual spend made by the Customer,

5.7.3 a summary of all products consumed with a growth/decline profile across the year,

5.7.4 a review of all recorded outages, risks and issues and plans for resolving any outstanding issues.

Invoicing

6.1 The Supplier shall provide invoices to the Customer.

6.2 The Invoices shall contain the following information at a minimum:

6.2.1 A valid Purchase Order number

6.2.2 Consumption MI detailing a breakdown of all service and products provided

6.2.3 Product details and associated costs

6.2.4 VAT number

6.2.5 VAT charges

6.2.6 Agreement number

6.2.7 Service Credits

6.3 The supplier shall provide Invoices to the Customer on a monthly basis within 10 days of the previous month end and payment shall be made within 30 days of confirmed receipt.

6.4 Any Invoices submitted by the Supplier that do not have an associated Purchase Order number(s) and accurate quantities, product details and associated costs shall be considered to be invalid by the Customer and shall be rejected accordingly.

6.5 All Invoices submitted by the Supplier shall contain both Purchase Order numbers, associated Agreement number and any relevant project reference number where applicable.

6.6 All Invoices must be in £ sterling

6.7 The Supplier shall provide further documentation to substantiate the Invoice (Invoice Report).

6.8 If the Supplier or the Cloud Provider enter into a Sub-Contract with another third party for the provision of any product or service provided to the Customer the Supplier must inform the Customer before such an arrangement is made. In such circumstances the Supplier must ensure that a provision is included in each

Subcontract which specifies that payment shall be made to the subcontractor within 30 days of receipt of any valid invoice.

6.9 The Supplier will indemnify the Customer on demand against any liability arising from the Suppliers failure to account for or pay any VAT on payments made to the Supplier for services or products provided. The Supplier shall pay all sums to the Customer with at least 5 working days before the date on which the tax or liability is payable by the Customer.

6.10 The Supplier shall not suspend supply of services or products unless the Supplier is entitled to under any relevant termination terms of the SCE

6. Training and Consultancy

7.1 The Supplier shall facilitate the Customer getting access to Subject Mater Experts (SME) from the Cloud Provider.

7.2 The SME access shall be made available throughout the contract to assist in the procurement of further cloud environments and associated software across a variety of cloud suppliers brining market knowledge to the Customer in order for he Customer to exploit and take advantage of latest industry developments.

7.3 The SME access shall be available throughout the contract to assist in the development and execution of plans to migrate existing applications and workloads from the om premise hosting and other cloud providers platforms into the Cloud Provider platform.

7.4 The Supplier must provide and manage the use of the Training Credits available to the Customer.

7.5 The Supplier shall support the Customer with making appropriate templates, processes, patterns etc. for shared services ensuring these are available from the outset, tailored to the Customer requirements and compliant with the Customers security and other design standards, whilst ensuring cloud optimisation from initiating the service, not beyond.

7.6 Front door access for the Customers product development units shall have a set of prepared artefacts for entry including standard sizing and acknowledgement requirements.

Schedule 2: Call-Off Contract charges

1. For each individual Service, the detailed Charges breakdown for the provision of Services during the Term will include:

   [Redacted]

2. The Call-Off charges will be agreed monthly in line with the Buyers consumption of the Microsoft Azure service. The Supplier will provide monthly billing MI to outline applicable Call-Off Charges.

3. The Suppliers service offering can be found at: https://www.applytosupply.digitalmarketplace.service.gov.uk/gcloud/services/496633533699259

4. [Redacted]

5. [Redacted]

6. [Redacted]

Schedule 3: Service Levels and Service Management Governance

SERVICE LEVELS (SLA)

Microsoft SLAs

1.1 Microsoft are the responsible party for the service level targets, measurements and service credits set out in clauses 1.1 through 1.8 in accordance with the Microsoft Licensing terms. Service credits will not apply to any failure to meet the uptime/availability service levels which are the result of or have been impacted by an action, or inaction, by the Buyer or any of the Buyer third party.

1.2 The service levels applicable are as published through the link below, some of which are subject to the Microsoft Azure resources being consumed by the Buyer:

1.2.1 Link to the Microsoft SLA's:

https://azure.microsoft.com/en-gb/support/legal/sla March 2023 embedded:

1.3 The following Microsoft published SLA's will apply to the Azure hosting services, but have been stated in this schedule for clarity and visibility, but not limited to:

1.3.1 Incident Response - Link to the Microsoft SLA's: https://azure.microsoft.com/engb/support/plans/response/

1.3.2 Uptime (availability) - Link to the Microsoft SLA's: https://azure.microsoft.com/en-gb/support/legal/sla/virtual-machines/v1_9/

INCIDENT RESOLUTION SERVICE LEVELS

TABLE 1 – INCIDENT PRIORITY LEVEL DEFINITIONS

Incident Priority Level	Classification	Business Impact

Severity A	Customer's business has significant loss or degradation of services and requires immediate attention.	• No immediate workaround is available. • Service unavailable to the vast majority of users. • Vital business function(s) severely impacted.
Severity B	Customer's business has moderate loss or degradation of services, but work can reasonably continue in an impaired manner.	• No immediate workaround is available. • Service functionality or performance is severely impaired. • Majority of users are unable to access the service. • Vital business function(s) impacted.
Severity C	Customer's business is functioning with minor impediments of services.	• A workaround is available. • Functionality or performance is degraded but the service is still usable. • More than 75% of users are able to access the service with no significant impact. • Vital business function(s) are not impacted.

TABLE 2 – INCIDENT RESPONSE TIME

SEVERITY LEVEL	CUSTOMER'S SITUATION	INITIAL RESPONSE TIME	EXPECTED CUSTOMER RESPONSE	SERVICE LEVEL REQUIREMENT
Severity A	**Critical business impact** Customer's business has significant loss or degradation of services and requires immediate attention. [3]	Premier: < 1 hr 24/7 access	When you select Severity A, you confirm that the issue has a critical impact on your business, with severe loss and degradation of services. The issue demands an immediate response, and you commit to continuous 24/7 operation every day with the Microsoft team until resolution; otherwise, Microsoft may at its discretion decrease the severity to level B. You also ensure that Microsoft has up-to-date contact information.	**MICROSOFT GUARANTEE RESPONSE TIMES**

Severity B	**Moderate business impact** Customer's business has moderate loss or degradation of services, but work can reasonably continue in an impaired manner.	Premier: < 2 hr Business hours access (24/7 available)	When you select Severity B, you confirm that the issue has a moderate impact on your business, with loss and degradation of services, but with workarounds that enable reasonable, albeit temporary, business continuity. The issue demands an urgent response. If you chose 24/7 when you submit the support request, you commit to a continuous 24/7 operation every day with the Microsoft team until resolution; otherwise, Microsoft may at its discretion decrease the severity to level C. If you chose working hours support when you submit a Severity B incident, Microsoft will contact you during working hours only. You also ensure that Microsoft has up-to-date contact information.	

SEVERITY LEVEL	CUSTOMER'S SITUATION	INITIAL RESPONSE TIME	EXPECTED CUSTOMER RESPONSE	SERVICE LEVEL REQUIREMENT
Severity C	**Minimum business impact** Customer's business is functioning with minor impediments of services.	Premier: < 4 hr Business hours access	When you select Severity C, you confirm that the issue has a minimum impact on your business, with a minor impediment to service. For a Severity C incident, Microsoft will contact you during working hours only. You also ensure that Microsoft has up-to-date contact information.	

UPTIME (AVAILABILITY) SERVICE LEVELS

1.4 The following published SLA's will apply to the Services, but have been stated in this schedule for clarity and visibility:

1.4.1 Uptime (availability) - Link to the Microsoft SLA's:

https://azure.microsoft.com/en-gb/support/legal/sla/virtual-machines/v1_9/

1.5 The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines, deployed across two or more Availability Zones in the same region:

TABLE 3.1

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%
< 95%	100%

1.6 The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines in an Availability Set, or same Dedicated Host Group:

TABLE 3.2

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%
< 95%	100%

1.7 The following Service Levels and Service Credits are applicable to Customer's use of Single-Instance Virtual Machines:

TABLE 3.3

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%
< 95%	100%

Service Credits Relating To Uptime (Availability)

1.8 In accordance to Microsoft published SLA document, see link below, the Service Credit percentage is used as below to calculate the monetary value of the service credit due to the Customer:

1.8.1 Service Credit is the percentage of the Applicable Monthly Service Fees credited to the Customer following Microsoft's service credit claim approval

1.8.2 Applicable Monthly Service Fees means the total fees actually paid by the Customer for a Service that are applied to the month in which a Service Credit is owed.

1.8.3 Microsoft and the Customer work together to apply the various calculations as stated in the Microsoft published SLA document, see link below, to calculate downtime and service credit implications

https://azure.microsoft.com/en-gb/support/legal/sla

March 2023 embedded:

Supplier Service Wrap SLAs

1.9 The Supplier will appoint a service delivery lead who will be responsible for managing the contract, reporting, attending service reviews and providing a continued service improvement plan that ensures that the service evolves and improves throughout the life e.g. refining processes.

1.10 The following Services Levels in this schedule are in addition to the Microsoft support published SLA's, which apply to the Supplier services:

1.10.1.1 Service Management and Governance

1.10.1.2 Provide reporting on Optimisation & Reserved Instance Optimisation **OPTIMISATION SERVICE LEVELS**

On-demand and Reserved Instance Optimisation

1.11 The Buyer and the Supplier will agree Optimisation targets through the service management process.

TABLE 4 - ON-DEMAND AND RESERVED INSTANCE OPTIMISATION REVIEW

Measurement	Service Level Requirement
The Supplier shall provide an optimisation report detailing areas that the Buyer needs to focus on and the actions to be taken. The details of the optimisation report are stated in table 5 below. This report shall be provided once a month in line with the Service Management – Service Reporting timetable stated in Table 6 and is subject to 1.13	100%

Remedies Relating To Optimisation

1.12 The standard provisions for dispute resolution and material breach will apply as set out in this Call Off Contract and the GCloud 13 Framework Agreement ref. RM 1557.13

OPTIMISATION SERVICE LEVEL COMMITMENTS

1.13 The Supplier will provide a report that details a benchmark against Cloud Intelligent Service (CIS) to enable the Buyer to enact process improvement. Where commercially and technically viable the Supplier will work with the Buyer as per the agreed governance process. Any changes to the suppliers proposed platforms and scope will be subject to agreement between the Parties, both acting reasonably, and may incur additional charges.

1.14 Any such charges will be subject to the variation process of this contract. A Roles Accountability Consult and Inform (RACI) which explains who owns the provision of the data e.g., Customer, Supplier or Microsoft via Supplier access will be agreed from 60 (sixty) days of the Call-Off signatures.

1.15 The below is to form a basis of the Azure estate monthly improvement recommendations and service improvements.

TABLE 5 - OPTIMISATION REPORTS

Area		Descriptor

Area of Focus	→	Reservations – Following the effective rightsizing of the Buyer VMs by the Buyer, the Buyer can request quotes for the purchase of reserved instances. The Supplier will make sure that these have been provided and support the evaluation as the next step. Quotes can be amended upon a Buyer request to ensure that requirements are met.
Reports	→	Supplier CIS are to share all optimisation reports with the Buyer designated Microsoft Azure service manager.
Policies	→	Supplier CIS to recommend to the Buyer on what policies the Buyer would benefit from.
Rightsizing	→	The Supplier CIS to continue monitoring the Buyer Microsoft Azure arrangements for current workloads and for any new assets that are created and advise the Buyer on how to balance cost and performance

SERVICE MANAGEMENT & GOVERNANCE SERVICE LEVELS

1.16 These are governance-based service levels for good industry practice in managing a strategic relationship between the Customer and the Supplier.

1.17 The Supplier will work in collaboration with the Customer to define the detail reports supporting the governance meetings in Table 6. This should include a Roles Accountability Consult and Inform (RACI) which explains who owns the provision of the source data e.g., Customer, Supplier or Microsoft via Supplier access. This needs to be agreed from 30 (thirty) days of the Call-Off signatures.

TABLE 6 – SERVICE MANAGEMENT

Service Element	Service Type	Cut Off Time and Other Matters
Pre-agreed ad-hoc Service Management – Service Reporting	Formal service delivery committee supported by pre-agreed ad-hoc reports	Within the pre-agreed timeframe from point of the Buyers request.
Service Management – Service Reporting (Monthly)	Formal service delivery committee supported by monthly reports	Within 48hrs of the calendar month end and less than 5 Working Days prior to the scheduled times for service delivery meeting.
Service Management – Service Delivery Meetings	Quarterly committee meetings as defined in the operating Governance Model to be agreed by both Parties (offsite via conference call)	Rescheduled meetings within 5 Working Days of the scheduled times
Service Management – Service Delivery Meeting Minutes	Meeting minutes for all governance meetings as defined in the operating Governance Model to be agreed by both Parties	3 Working Days for the Supplier to issue the minutes to Customer plus a further 2 Working Day for Customer to agree.
Service Management – Responsiveness	Availability to Customer of the Supplier Service lead or delegate(s) as per the defined escalation path	Supplier Service lead or delegate(s) is available to Customer as per the defined escalation path within 1 working day of contact initial contact by Customer.

Remedies Relating To Service Management

1.18 The standard provisions for dispute resolution and material breach will apply as set out in this Call Off Contract and the GCloud 13 Framework Agreement ref. RM 1557.13.

Appendix 1 – MINIMUM SECURITY REQUIREMENTS

GENERAL

The Contractor shall and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Appendix 1 to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this Appendix 1 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this Appendix 1, the following definitions shall apply:

"Authority Personnel"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Contractor and any Sub-contractor (as applicable).
"Availability Test"	shall mean the activities performed by the Contractor to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.

"**Cyber Essentials**"		shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Cyber Security Information Sharing Partnership**" or "**CiSP**"		shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Good Security Practice**"	b)	shall mean: the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology);
	c)	security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and
	d)	the Government's security policies, frameworks, standards and guidelines relating to Information Security.
"**Information Security**"		shall mean:
	b)	the protection and preservation of:

iv) the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor's Systems Environment (or any part thereof);

v) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and

c) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.

"**Information Security Manager**"	shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority's Security Requirements.
"**Information Security Management System ("ISMS")**"	shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor to manage Information Security Risk as specified by ISO/IEC 27001.
"**Information Security Questionnaire**"	shall mean the Authority's set of questions used to audit and on an ongoing basis assure the Contractor's compliance with the Authority's Security Requirements.
"**Information Security Risk**"	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
"**ISO/IEC 27001, ISO/IEC 27002** d) **and ISO 22301** e)	shall mean ISO/IEC 27001; ISO/IEC 27002/IEC; and

f) ISO 22301	in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.
"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Penetration Test**"	shall mean a simulated attack on any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof).
"**PCI DSS**"	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "**PCI**").
"**Risk Profile**"	shall mean a description of any set of risk. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof).

1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority's Representative.

2. PRINCIPLES OF SECURITY

2.1 The Contractor shall at all times comply with the Authority's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Contract);
b) a risk assessment (which shall include any risks specific to the Services);
c) a statement of applicability;
d) a risk treatment plan; and
e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

3.4 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.

3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such noncompliance. The Contractor shall, at its own expense, undertake those actions required in order to comply with the Authority's

Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause 18.5.

4. RISK MANAGEMENT

4.1 The Contractor shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority's Security Requirements are met (the **Risk Assessment**). The Contractor shall provide the Risk Management Policy to the Authority upon request within 10 Working Days of such request. The Authority may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Authority's Security Requirements. The Contractor shall, at its own expense, undertake those actions required in order to implement the changes required by the Authority within one calendar month of such request or on a date as agreed by the Parties.

4.2 The Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Contractor shall notify the Authority within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

4.3 If the Authority decides, at its absolute discretion, that any Risk Assessment does not meet the Authority's Security Requirements, the Contractor shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

4.4 The Contractor shall and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.

4.5 For the avoidance of doubt, the Contractor shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph **Error! Reference source not found.**. Any failure by the Contractor to comply with any requirement of this paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy), shall

constitute a Material Breach entitling the Authority to exercise its rights under clause 18.5.

5. SECURITY AUDIT AND ASSURANCE

5.1 The Contractor shall and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

5.2 The Contractor shall conduct Security Tests to assess the Information Security of the Contractor's Systems Environment and, if requested, the Authority's Systems Environment. In relation to such Security Tests, the Contractor shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the Authority's System Environment or (iii) at the request of the Authority which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Authority. The Contractor shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Contractor shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Authority in its absolute discretion.

5.3 The Authority shall be entitled to send the Authority's Representative to witness the conduct of any Security Test. The Contractor shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.

5.4 Where the Contractor provides code development services to the Authority, the Contractor shall comply with the Authority's Security Requirements in respect of code development within the Contractor's Systems Environment and the Authority's Systems Environment.

5.5 Where the Contractor provides software development services, the Contractor shall comply with the code development practices specified in the Specification or in the Authority's Security Requirements.

5.6 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor shall, at its own expense, undertake those actions required in order to rectify such identified

noncompliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

5.7 The Authority shall schedule regular security governance review meetings which the Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

6. PCI DSS COMPLIANCE AND CERTIFICATION

6.1 Where the Contractor obtains, stores, processes or transmits payment card data, the Contractor shall comply with the PCI DSS.

6.2 The Contractor shall obtain and maintain up-to-date attestation of compliance certificates ("**AoC**") provided by a qualified security assessor accredited by the PCI and up-to-date self-assessment questionnaires ("**SAQ**") completed by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the "PCI Reports"), during the Contract Period. The Contractor shall provide the respective PCI Reports to the Authority upon request within 10 Working Days of such request.

6.3 The Contractor shall notify the Authority of any failure to obtain a PCI Report or a revocation of a PCI Report within 2 Working Days of confirmation of such failure or revocation. The Contractor shall, at its own expense, undertake those actions required in order to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

7. SECURITY POLICIES AND STANDARDS

7.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.

7.2 Notwithstanding the foregoing, the Authority's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

7.3 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

8. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

8.1 The Supplier may require a nominated representative of the Supplier to join the Cyber Security Information Sharing Partnership on behalf of the Supplier during the Term, in which case the Supplier's nominated representative shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

8.2 If the Supplier elects a nominated representative to join the Cyber Security Information Sharing Partnership in accordance with Paragraph 8.1 above, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-securitypolicies-and-standards unless specified otherwise:

2. Acceptable Use Policy

3. Information Security Policy

4. Physical Security Policy

5. Information Management Policy

6. Email Policy

7. Technical Vulnerability Management Policy

8. Remote Working Policy

9. Social Media Policy

10. Forensic Readiness Policy

11. SMS Text Policy

12. Privileged Users Security Policy

13. User Access Control Policy

14. Security Classification Policy

15. Cryptographic Key Management Policy

16. HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnelsecurity-controls)

17. NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on: https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

b) SS-001 - Part 1 - Access & Authentication Controls
c) SS-001 - Part 2 - Privileged User Access Controls
d) SS-002 - PKI & Key Management
e) SS-003 - Software Development
f) SS-005 - Database Management System Security Standard
g) SS-006 - Security Boundaries
h) SS-007 - Use of Cryptography
i) SS-008 - Server Operating System
j) SS-009 - Hypervisor
k) SS-010 - Desktop Operating System
l) SS-011 - Containerisation
m) SS-012 - Protective Monitoring Standard for External Use
n) SS-013 - Firewall Security
o) SS-014 - Security Incident Management
p) SS-015 - Malware Protection
q) SS-016 - Remote Access
r) SS-017 - Mobile Devices
s) SS-018 - Network Security Design
t) SS-019 - Wireless Network
u) SS-022 - Voice & Video Communications
v) SS-023 - Cloud Computing
w) SS-025 - Virtualisation
x) SS-027 - Application Security Testing
y) SS-028 - Microservices Architecture
z) SS-029 - Securely Serving Web Content aa) SS-030 - Oracle Database bb) SS-031 - Domain Management cc) SS-033 - Patching

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) 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 Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	For each Party, IPRs: owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.

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

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.

Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
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	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR 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.

Data Subject	Takes the meaning given in the UK GDPR
Default	Default is any: breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
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 the outcome screen of the ESI tool.

Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most uptodate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: acts, events or omissions beyond the reasonable control of the affected Party riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare acts of government, local government or Regulatory Bodies fire, flood or disaster and any failure or shortage of power or fuel industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).

Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of 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.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
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.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium a Dun & Bradstreet rating of 10 or less

Intellectual Property Rights or IPR	Intellectual Property Rights are: copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: the supplier's own limited company a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	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 Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
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 Schedule 6.
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 UK GDPR.

Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: induce that person to perform improperly a relevant function or activity reward that person for improper performance of a relevant function or activity commit any offence: ○ under the Bribery Act 2010 under legislation creating offences concerning Fraud ○ at common Law concerning Fraud committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.

Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation 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 highperformance 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).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

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 GCloud 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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.

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-controlscheck-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 GCloud 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	The person, firm or company identified in the Order Form.
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: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

Annex 1: Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: [Redacted]

1.2 The contact details of the Supplier's Data Protection Officer are: [Redacted]

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Buyer is Controller, and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller, and the Supplier is the Processor of the Personal Data recorded below The Supplier will process the names and business contact details of the Buyer's staff in order to process this transaction. **The Supplier is Controller and the Buyer is Processor**

	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 16 of the following Personal Data: business contact details of the Buyer's staff in order **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: ***Not applicable.*** **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: *Business contact details of Supplier Personnel for which the Supplier is the Controller,* and *Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller.*

Duration of the Processing	Up to 7 years after the expiry or termination of the Framework Agreement
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this Framework Agreement including Ensuring effective communication between the Supplier and CSS Maintaining full and accurate records ofevery Call-Off Contract arising under the Framework Agreement in accordance with Clause 7.6
Type of Personal Data	Includes: i. Contact details of, and communications with, CSS staff concerned with management of the Framework Agreement

	Contact details of, and communications with, Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement,

Categories of Data Subject	Includes: CSS staff concerned with management of the Framework Agreement Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Agreement
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or	All relevant data to be deleted 7 years after the expiry or termination of this Framework
Member State law to preserve that type of data	Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder