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

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	[REDACTED]
Call-Off Contract reference	22053
Call-Off Contract title	Provision of Cloud Video Platform (CVP) services for the MoJ and HMCTS
Call-Off Contract description	Provision of Cloud Video Platform (CVP) services for the MoJ and HMCTS Provision of Video Hearings Services for HMCTS This Order Form does not commit the Buyer to spend any value under this Call-Off Contract. Commitment to spend shall be made via a countersigned CCN or Statement of Work, subject to approval from the Buyer.
Start date	1st April 2023
Expiry date	31st March 2025
Call-Off Contract value	£6.988m This Order Form does not commit the Buyer any value under this Call-Off Contract.
Charging method	BACS, 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	**The Secretary of State for Justice** Buyer's Main Address: 102 Petty France, London, SW1H 9AJ
To the Supplier	**AVMI Kinly Ltd** Supplier's Address: Europe House 170 Windmill Road West Sunbury on Thames Middlesex TW16 7HB Company number: 02468436

Principal contact details

It should be noted that whilst the Buyer is the Ministry of Justice (MoJ) this contract will be utilised by both the MOJ and its executive agency, His Majesty's Courts and Tribunal Service (HMCTS).

[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **1 April 2023** and is valid for **24 months.**
Ending (termination)	The Buyer shall not End this Call-Off Contact without cause (as per clause 18.1) prior to 31 March 2024. Subsequent to 31 March 2024 the notice period for Ending the Call Off Contract shall be 90 Working Days from: (a) In the case of the Supplier, the date of written notice for undisputed sums (as per clause 18.6) (b) In the case of the Supplier from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **2 months** written notice before its expiry (the 'Extension Notice'). The extension period is subject to clauses 1.3 and 1.4 in Part B below. In the Extension Notice the Buyer shall be entitled to specify that the extension is for CVP Services only and Video

	Hearings Services are not required during such extension period.

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 3: Cloud support
G-Cloud Services required	The Services to be provided by the Supplier are listed in: • Framework Schedule 4 • The Suppliers G-Cloud 13 Service Offering as set out in the Suppliers Service Description under reference 875152189530533 • Schedule 1 to this Call-Off Contract
Additional Services	Additional services, or variations (including reductions) to the Services as set out above, may be agreed following the approval of a Statement of Work.
	Services shall be delivered to:

Location	[REDACTED] and in courts and tribunals sites across the England and Wales and in certain reserved tribunals in Scotland.
Quality Standards	The quality standards required for this Call-Off Contract are as per the Supplier's G-Cloud 13 service offering 875152189530533. The Supplier shall ensure that the Supplier personnel shall during the Call-Off Contract period: - Be appropriately experienced, qualified, and trained to supply the services, in accordance with this Call-Off Contract. - Apply all due care, skill, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of those Services. - Have undergone a pre-employment check to the standard of HMG Baseline Personnel Security Standard (BPSS) or equivalent. The Supplier shall also ensure that its suppliers and all personnel with access to system code, or directly handling (e.g., transporting) large volumes of security classified data, shall be cleared to SC (Security Check) level.
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are as set out below. The Supplier shall deliver the Service in line with the Technology Code of Practice as specified by the G-Cloud framework and the following: • ISO 27001 Certification, covering the scope of the Service. • Software – The end-to-end service, including software and hardware/infrastructure must be subject to an annual Penetration test by

<table>
<tr>
<td></td>
<td>
CHECK approved testers.

• Annual IT Health checks (or at more frequent intervals if required). The Supplier to address any remediation required for identified vulnerabilities.

• Adherence to NCSC guidance (National Cyber Security Centre - the Government central authority for cyber security) must be provided and maintained throughout the duration of this Call-Off Contract.

• Compliance to Web Content Accessibility Guidelines (WCAG).

In addition to the above the Supplier shall undertake regular risk assessment (at least once every 6 months) of the Service and undertake all necessary remediation of identified risks.

All data shall be hosted in the UK
</td>
</tr>
<tr>
<td>Service level agreement:</td>
<td>
The service level and availability criteria required for this Call-Off Contract are as per the Supplier's G-Cloud 13 service offering 875152189530533.

A summary of the Service requirements set out below. Further details are set out in Schedule 1.

The Service Levels are:

<table>
<tr><th>Incident Priorities</th><th>Resolution Times</th></tr>
<tr><td></td><td></td></tr>
<tr><td>Priority 1 Incident – High</td><td>4 Hours</td></tr>
<tr><td>Priority 2 Incident - Normal</td><td>6 Hours</td></tr>
<tr><td>Priority 3 Incident - Low</td><td>8 hours (weekdays 08:00-17:00)</td></tr>
</table>

Definitions of above Incident Priorities

<table>
<tr><th>Incident Priorities</th><th>Definition</th></tr>
</table>
</td>
</tr>
</table>

Priority 1 Incident – High	The service is unavailable
Priority 2 Incident - Normal	The service is functioning but is impaired
Priority 3 Incident - Low	The service is functioning normally, but information or assistance is required

The Supplier shall.:

- Maintain a log of all calls; opening a ticket for new faults and providing case reference where applicable
- Provide technical support between 8:30 AM and 18:00 PM Mon-Fri (except when closed for public holidays).

Availability

- Service availability of 99.25%.
- Software shall be available and supported on a 24/7/365 basis.
- Software versions to be maintained as *n*-2 or later depending on security vulnerabilities, subject to Buyer and Supplier reviews.

Other Service Activities

The Supplier shall:

- Escalate any performance issues with the Service to the Buyer.
- Keep the Buyer involved and informed regarding all aspects of the Service provided.
- Undertake a formal review of the Service services monthly.

Onboarding	As the Supplier is the current incumbent supplier for this Service it is not anticipated that any specific

	onboarding activity will be required.

Offboarding	Within 6 months of the Start Date for this Call-Off Contract the Supplier shall provide the Buyer with an Exit Plan in accordance with Clause 21. This shall be reviewed and updated every 6 months with the intention that plans will be in place to minimise any adverse impact on service continuity at the end of this Call-Off Contact.
Collaboration agreement	A formal collaboration agreement is not required. The Buyer and Supplier shall build an open, honest, and transparent working relationship.
Limit on Parties' liability	As set out in clause 24.1
Insurance	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract. ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law). ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.

Buyer's responsibilities	The Buyer is responsible for**:** • Site access, including provision of security passes or escorting where required. • Reporting all technical issues to the Supplier in a timely manner using appropriate channels. • Escalating any service or performance issues through the appropriate escalation process. • Keeping the Supplier involved and informed regarding all aspects of the Service. • Providing reasonable support to the Supplier in obtaining security clearances beyond the level of BPSS as required for some personnel.
Buyer's equipment	Not applicable

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners [REDACTED]

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	**MoJ Invoices** Invoices will be sent to Email: MoJ Corporate Email: APinvoices-MOJ-U@gov.sscl.com Ministry of Justice PO Box 743 Newport Gwent NP10 8FZ **HMCTS Invoices** Invoices will be sent by email to: [REDACTED] A copy of all invoices should be sent to the Buyers Commercial Manager at the same time as they are submitted to the above.
Invoice information required	All invoices must include: - Contract reference number and title - Purchase order number - Invoice period - Description of services provided - Details of milestones and achievement date
Invoice frequency	Invoices will be sent to the Buyer monthly.
Call-Off Contract value	The total value of this Call-Off Contract is £6.988m (six million and nine hundred and eighty-eight thousand pounds)

Call-Off Contract charges	[REDACTED]

Additional Buyer terms

Performance of the Service	Monthly meetings shall be held to monitor performance. The Supplier shall collect and report on the following: • Volume of calls (split between MoJ and HMCTS) • Percentage uptime of service (measured against the availability percentage 99.25%) for CVP and VHS • Delivery against all Service levels. • Security update. • Invoicing information. • Monthly utilisation In addition to the above the Supplier shall highlight to the Buyer any ideas for the co improvement of the service. The amount of compute time used shall be reported on a weekly basis. The Supplier agrees that the following three key performance indicators will be repo monthly basis and the Buyer shall be entitled to publish the performance levels in ac with obligations to the Cabinet Office:

Description	Target
Participants using the cloud video platform and video hearings	>99.25%

	<table><tr><td>service should be able to access the service at least 99.25% of the time during core working hours</td><td></td></tr><tr><td>Resolution of Priority 1 incidents (where the service is unavailable)</td><td><4 hours</td></tr><tr><td>Training provided to apprentices and work experience offered to school leavers</td><td>Details to be finalised within 30 days of the date of this Contract.</td></tr></table>
Guarantee	Not required
Warranties, representations	In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants and represents to the Buyer that all data will be hosted in the UK.
Supplemental requirements in addition to the Call-Off terms	Not applicable
Alternative clauses	Not applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	Please refer to Special Term 7.13 which has been added to the standard Call-Off Contract terms

Personal Data and Data Subjects	Annex 1 of Schedule 7 is being used
Intellectual Property	As per standard Call-off Contract terms
Social Value	The Social Value requirements are set out in Schedule 1.

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

Signed	Supplier	Buyer
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)

- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- 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:

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

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

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

2.3 The 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.

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

2.5 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 G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed 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.

7.13 **Adjustment to Call-Off Contract Charges** [*Special Term*]

7.13.1 Any Call-Off Contract Charges in this Call-Off Contract which are expressed to be "subject to indexation" shall be adjusted in accordance with the provisions of this Special Term 7.13 to reflect the effects of indexation.

7.13.2 The relevant adjustment for indexation (which could be an increase or decrease) shall be:

(a) applied six (6) months from the start date of the Call-Off Contract and every six (6) months thereafter (each such date an "**adjustment date**") until the expiry or termination of the Call-Off Contract; and

(b) determined by multiplying the Call-Off Contract Charges set out in the Schedule 2 by the percentage increase or decrease in the Consumer Price Index during the six (6) months immediately preceding the adjustment date.

7.13.3 Except as set out in Special Term 7.13.2, neither the Call-Off Contract Charges nor any other costs, expenses, fees or charges shall be adjusted for changes to any inflation, exchange rates, interest rates or any other factor or element even if there is an increase in costs to the Supplier and/or its Sub-contractors in performing their obligations set out in the Call-Off Contract.

7.13.4 During the Framework Agreement Term, including any extensions, any adjustment to the Call-Off Contract Charges pursuant to Special Term 7.13.2 shall not be increased above the price quoted in the Supplier's Platform Application.

7.13.5 The indexation provision shall not be applied to adjust rates which have been pre-booked.

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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 employer's 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. If there are any additional insurance policies required by the Buyer, this may be subject to additional charges form the Supplier.

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 trade marks 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:

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;

(c) 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:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 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:

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

11.7.2 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

11.7.3 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:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 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 G-Cloud 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-policy-framework and the Government Security Classification policy: https:/www.gov.uk/government/publications/government-securityclassifications

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

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

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-of-practice/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-security-principles

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-of-practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 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 – not required

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 an alternative 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 Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

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

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

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

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

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:

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

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

19.5.3 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

19.5.4 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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- 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 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks but preferably 90 days before the end of the requested extension period.

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

29.2.11 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

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

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

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

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

29.5.1 its failure to comply with the provisions of this clause

29.5.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

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

29.7 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

[REDACTED]

Annex A

[REDACTED]

Annex 2: Template for the Service Management Plan

Security Management Plan

Version *{insert}*

Date

This is a template for a document to be produced by the supplier to explain how their ISMS is applied to the information security requirements placed upon them by HMCTS.

There are two types of helpful suggestions included in this template. Where it is judged that text is likely to be boilerplate it is in normal font; suppliers are requested to review such text

in the light of their solution and delete, modify and/or add to it as appropriate. Where the contents are likely to be more solution dependent a prompt as to the expected content is given.

The document presented is expected to be devoid of all blue italicised material and to be the standalone SMP from the supplier.

Document History

Version	Date	Comments

Document References

Ref	Title
A	
B	

Abbreviations & Glossary

Title	Definition

Engagement Details (Supplier use only)

Agreement Name	

Introduction

Purpose

This document is the baseline Security Management Plan (SMP) to be used by *Name of Supplier* (hereafter referred to as "Supplier") for the work undertaken for the HM Courts and Tribunals Service (hereafter referred to as 'the Buyer') under Agreement reference *xxxxx* [A].

The SMP sets out the security controls to be implemented and maintained by the Supplier in relation to the security aspects and processes associated with the delivery of its services to the Buyer ("the Services").

The Supplier implements, operates, maintains and continuously improves an Information Security Management System (ISMS). In line with this the Supplier has developed and maintains an SMP. *The Supplier's ISMS is certified compliant with the requirements of International Standards Organisation (ISO) 27001:2013 [B] by the {Insert certifying body}. (If true – the supplier may not be contractually required to be ISO27001 certified. If not true, the supplier still has to have an ISMS whose scope encompasses the service provided).*

The Supplier shall comply with its obligations set out in the SMP.

Scope

Both the ISMS and the SMP shall, unless otherwise specified by the Buyer, aim to protect all aspects of the Services and all processes associated with the delivery of the Services, including Buyer Premises, the Sites, the Supplier System and any information and communication technology (ICT), information and data (including Buyer Confidential Information and Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Agreement.

The scope of The Supplier's work is illustrated in Figure 1 below.

Insert figures as appropriate

Figure 1 - Scope

The SMP is not intended to define or document the operational processes, procedures, or associated work instructions or documentation records to be deployed for HMCTS.

Approval of the SMP

If the SMP, or any subsequent revision to it, is approved by the Buyer, it will be adopted immediately. If the SMP is not approved by the Buyer, the Supplier shall amend it within 5 Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for approval. The parties will seek to ensure that the approval process takes no longer than 10 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the Buyer.

1.4 Content of the SMP

The SMP sets out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall always comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions set out in the Agreement.

Specifically, the SMP:

- Sets out the security controls to be implemented and maintained by the Supplier in relation to security requirements and processes associated with the delivery of the services to be delivered under the agreed contractual terms.
- Demonstrates that the security policies, controls, procedures and services provisioned comply with the provisions and principles set out in line with the relevant client and regulatory framework.
- Aims “to protect the aspects of the services and the processes associated with the delivery of the Services, including the Buyer premises, the sites, the contractor system and any ICT system.”

The security controls and procedures set out in this document demonstrate that the Services provided comply with the provisions and principles set out in the Agreement reference *xxxxx* [A].

It is the responsibility of the Buyer to notify the Supplier, through the review process for this document, of any required controls above and beyond those detailed in this document or of any changes required to the baseline security controls detailed in this document. If no notification is provided the Buyer acknowledges that the baseline security controls detailed in this document are adequate.

Buyer Responsibilities

The Buyer will:

- Promptly notify the Supplier of any security risks, policies or procedures relevant to the Services that require additional security controls in addition to those listed below;
- Have robust and adequate security arrangements with respect to the receipt of the Services;
- Be responsible for the adequacy of its security arrangements and for monitoring compliance against them;
- Undertake regular monitoring of this SMP; and
- Notify the Supplier in a timely manner of any proposed changes to their Security Policy and/or security requirements and the parties will then agree what consequential changes need to be made to this SMP.

Amendment and Revision

The SMP will be normally reviewed by the Supplier on an annual basis to reflect:

- Significant emerging changes relating to industry good practice;
- Any changes in Agreement or Framework requirements; and
- Any specific and agreed changes to security policy advised by the Buyer that impact the services.

The Supplier will provide the Buyer with the results of any reviews of this document and will only implement any proposed changes or amendments to the document following approval in writing by the Buyer. Any changes to the SMP requested by the Buyer will require the Supplier to be informed using Clause *xxxx* (Variation Procedure).

Processing, Storage and Classification

This section should:

- *Follow the Security Aspects Letter (SAL) in stating the maximum Government Security Classification attracted by the work.*
- *Explain that OFFICIAL can normally be processed and stored on the Supplier's standard corporate ICT infrastructure.*
- *Explain that where additional controls are required for some data classified at OFFICIAL-SENSITIVE and all data at higher classifications these will be described in this SMP.*

Security Roles & Responsibilities

The following table lists the Supplier's security roles, the expected security responsibilities and the name of the person(s) assigned to each role.

Security Roles and Assignments		
Security Role	**Name and Contact Information**	**Security Responsibilities**
Compliance Officer	Name: Title: Email address: Phone number:	
Chief Information Officer (CIO) – Board Member responsible for security	Name: Title: Email address: Phone number:	

Security Roles and Assignments		
Security Role	**Name and Contact Information**	**Security Responsibilities**
Configuration Management, Change Manager (CM)	Name: Title: Email address: Phone number:	
Contracts, Procurement Officer/Manager	Name: Title: Email address: Phone number:	
Contracting Officer's Technical Representative	Name: Title: Email address: Phone number:	
Information System Security Officer	Name: Title: Email address: Phone number:	
Information Technology Architect	Name: Title: Email address: Phone number:	

Security Roles and Assignments		
Security Role	**Name and Contact Information**	**Security Responsibilities**
Legal Advisor / Representative	Name: Title: Email address: Phone number:	
Privacy or Data Protection Officer	Name: Title: Email address: Phone number:	
Other Participants	Name: Title: Email address: Phone number:	

2 Staff Security Training & Awareness

The following table identifies the person responsible for assuring that training and education is provided to all parties responsible for performing security awareness activities as part of the application System's process.

Security Role	Name and Contact Information
Responsible Person	Name: Title: Email address: Phone number:

Explain how the supplier delivers security training at induction and refresher training annually.

Explain other forms of security training and security awareness undertaken.

1. 3 Risk Management

Describe your information risk management policy and process. Include how you categorise risk, capture risk, set tolerances, mitigate, accept risks etc.

Respond to any specific risk related requirements in the contract.

Security Controls

This section summarises the Supplier's Baseline Security Controls, in accordance with ISO 27001, which will be applied to the delivery of the services. Where the Buyer security requirements mean that additional controls or amendments to controls are needed, then this is detailed after the description of each control.

3.1 Security Policy

It is expected that the following words would apply to most organisations but modify as necessary.

All Staff and the Suppliers have an individual responsibility to ensure their personal compliance with the Supplier security policies within the ISMS.

Describe any security certifications which demand policy (eg ISO 27001); state who provides the certification and the frequency of review.

Supplier ICT operational procedures and the security controls documented in the security policies set are compliant with ISO 27001. The policies are approved by the Supplier senior management and are published for all Supplier staff and temporary workers to view. Furthermore, the Supplier reviews the policies annually and in response to significant changes or new threats (e.g. new risks, regulatory or legislative changes and new technological developments). All Supplier personnel, whether contractors or employees, are responsible for ensuring that Buyer and the Supplier confidential information, in whatever form, is handled securely and confidentially.

All Supplier staff, contractors and temporary workers are required to comply with the Supplier Security Policies. *Describe how this is achieved – eg induction training, continuation training, declaration that they will comply and easy access to the policies, SyOPs.*

3.2 Organisation of Information Security

3.2.1 Internal Organisation

It is expected that the following words would apply to most organisations but modify as necessary.

All queries regarding security for the delivery of Services are referred and escalated to the following individuals in the following order:

- The Supplier's Security Representative
- The Buyer's Security Representative.

The Supplier assigns responsibilities for security, seeks to understand the Buyer's policies, and communicates the relevant aspects to the Supplier team members in an effective way. Supplier team members and managers have accountability and responsibility respectively for the security of the Services delivered. Authority is delegated to *{insert}* for day-to-day compliance and, where appropriate, to the relevant project managers of any supporting sub-contractors. *Describe whether and how you separate roles and responsibilities where there is potential for malicious or accidental breach of information security. If this is impracticable (eg due to the small size of the team) describe any compensating controls.*

3.2.2 *Contract Purpose*

{Insert contract purpose}. A high-level risk assessment has been created and will be under continual review as the project moves forward. The security measures to manage the risks identified are dealt with in the remainder of this plan.

3.3 Human Resource Security

3.3.1 Prior to Employment

It is expected that the following words would apply to most organisations but modify as necessary.

The Supplier, and its partners, maintain formal personnel security procedures as part of their information security programme which include comprehensive background checks for all employees.

All employees acknowledge company policies, non-disclosure agreements (NDA), and other confidentiality agreements. Information security awareness training is mandatory; *explain how this is recorded and administered.*

Explain how you apply NCSC guidance on personnel security including how you conduct vetting and clearance. Ensure that this also covers your supply chain and state whether you sponsor third parties to obtain appropriate clearance.

3.3.2 During Employment

It is expected that the following words would apply to most organisations but modify as necessary.

All Supplier personnel are held responsible for the protection of Buyer information entrusted to them, or information to which they are otherwise exposed. As such, the Supplier project team should be aware of the engagement security requirements, understand their responsibilities and the need to adhere to all applicable Buyer security policies, procedures and standards to ensure compliance, and will be required to sign-off this process at the commencement of the engagement.

The Supplier has a clearly defined, documented disciplinary policy and procedures which are communicated to all employees. *Explain how this is available and how employees and contractors are reminded of its importance.*

Information security awareness is covered during new employee onboarding and additional training is provided to employees with privileged access.

Detail any extra controls required for this contract – eg any requirements for SC and how you will meet them, or any extra specific confidentiality undertakings.

3.3.3 Termination and Change of Employment

It is expected that the following words would apply to most organisations but modify as necessary.

Upon termination of employment, there is a process in place to ensure that individuals return any Supplier property in their possession. Access rights are removed automatically from Supplier systems when an individual's employment is terminated. On change of employment there is a process to ensure that only access rights relevant to the new role are retained.

3.4 Asset Management

3.4.1 Responsibilities for Assets

Your current asset management processes should be briefly described here.

Record any additional asset management information specific to this contract here.

3.4.2 Information Classification

The United Kingdom (UK) Government Security Classification System currently comprises three tiers of OFFICIAL, SECRET and TOP SECRET assets. The majority of government information assets fall into the first of these. In accordance with Cabinet Office guidance, information classified as OFFICIAL can be routinely managed within the Supplier's enterprise-level ICT systems and subject to controls aligned with the Supplier's *{insert certification, ISMS etc here}*. In summary, the following approach will be taken to hold and process Government Information Assets:

- **OFFICIAL –** The assets may usually be stored within the Supplier's standard corporate network unless the volume and sensitivity of the data demands an increased classification and additional controls. Data held on the Supplier's laptops are protected by Whole Disk Encryption and all personnel working on information at this level are required to hold a valid BPSS.

- **OFFICIAL-SENSITIVE** – Should the Buyer Senior Information Risk Owner (SIRO) seek additional controls for OFFICIAL-SENSITIVE the Supplier will work with Buyer security teams to agree appropriate risk mitigation and the implementation and management of any additional controls or processes.

Information assets will be treated in accordance with their classification and in accordance with any other requirements agreed between the Supplier and the Buyer throughout their life. *Record here how any contract specific information assets will be handled.*

Describe what will happen to the information assets at the end of the contract.

3.4.3 Media Handling

Describe how you control removable media within your IT estate.

Describe any particular extra, or changed, controls required for this contract.

3.5 Access Control

3.5.1 Business Requirements

It is expected that the following words would apply to most organisations but modify as necessary.

There are access control policies for both physical and logical access to information assets. These policies are supported by processes to ensure that access rights are aligned with user roles and the security risk assessment. In addition, the need to know principle is applied and the classification of information is considered in all access decisions. Access is formally granted by the asset owner, is reviewed on a regular basis and is withdrawn on change of need or termination of employment. The roles involved in the management of access are segregated.

3.5.2 User Access Management

It is expected that the following words would apply to most organisations but modify as necessary.

To achieve the requirements of paragraph 3.5.1, there are formal processes around the granting, monitoring and revoking of access. Privileged user access is strictly controlled to conform to a "need to use" basis and privileged access is only allowed through a different user ID than for general business activities.

Describe your user access management policies.

Describe any variations or additions for this contract.

3.5.3 User Responsibilities

User responsibility for protecting their passwords is covered in *{insert}.*

Describe any extra controls for this contract.

3.5.4 System and Application Access Control

Unauthorised access to systems and applications is restricted in accordance with the Supplier's *{insert}.*

Briefly describe your password management system and the controls surrounding it.

Briefly describe your privileged access management systems.

Describe any extra, or changed, controls for this contract.

3.6 Cryptographic Controls

It is expected that the following words would apply to most organisations but modify as necessary.

The Supplier has developed and implemented a Cryptography Policy which covers the circumstances under which encryption is mandatory. The policy also covers key management throughout the lifecycle of key material.

Describe any extra, or changed, controls for this contract.

3.7 Physical and Environmental Security

3.7.1 Secure Areas

Describe the physical security measures implemented at any locations involved in the provision of this contracts. Include perimeter measures, building measures, physical access mechanisms, CCTV, guarding, deliveries, despatches etc. Describe how these apply to this contract.

3.7.2 Equipment

Describe the physical security measures applicable to equipment. Include storage, printer use, storage of documents, environmental protection, UPS, power, telecommunications, remote working, decommissioning etc. Describe how these apply to this contract.

3.8 Operations Security

3.8.1 Operational Procedures and Responsibilities

There are documented operational procedures for all operational activities associated with information processing and communications.

Describe the security aspects of change management processes, capacity management, environment management etc.

Describe how these apply to this contract.

3.8.2 Protection from Malware

Describe how all systems are protected from malware. Describe how this applies to this contract.

3.8.3 Backup

It is expected that the following words would apply to most organisations but modify as necessary.

The Supplier has both policy and procedure for back-ups. Backups are logged, and the logs are held indefinitely. The Supplier implements multiple layers of redundancy and backup for business-critical systems such as database, email and storage. The Supplier's IT team can restore systems with up to date backups and this capability is regularly tested.

Describe any extra, or changed, controls for this contract.

3.8.4 Logging and Monitoring

Describe the protective monitoring used by the Supplier.

Describe how any requirements to provide protective monitoring to the Buyer will be met.

3.8.5 Control of Operational Software

It is expected that the following words would apply to most organisations but modify as necessary.

The installation of software on operational systems is strictly controlled to protect the integrity of the systems. The process ensures that appropriate authorisation is obtained, and that vendor supplied software is maintained and in support.

Describe any extra, or changed, controls for this contract.

3.8.6 Technical Vulnerability Management

Describe your policy and processes for technical threat and vulnerability management from recognition of threats and vulnerabilities through the risk management process to the remediation and testing of that remediation.

Describe any extra, or changed, controls for this contract.

3.8.7 Information Systems Audit Considerations

It is expected that the following words would apply to most organisations but modify as necessary.

Audit requirements (including external penetration and vulnerability testing) on operational systems are carefully controlled and subject to appropriate authorisation.

Describe any extra, or changed, controls for this contract.

3.9 Communications Security

3.9.1 Network Security Management

Describe the Supplier network security controls. Include controls relating to network service suppliers, how network service provision is monitored, network access controls, network segregation, visitor access etc.

Describe any extra, or changed, controls for this contract.

3.9.2 Information Transfer

It is expected that the following words would apply to most organisations but modify as necessary.

Personal responsibility for adherence to information transfer policies and procedures is reinforced in awareness training and through the medium of the *{insert here}* document. This is further enhanced by the SyOPs.

Describe the policy and processes used for the transfer of sensitive data. Describe any use of codes of connection if applicable.

Describe any extra, or changed, controls for this contract.

3.10 System Acquisition, Development and Maintenance

3.10.1 Security Requirements

It is expected that the following words would apply to most organisations but modify as necessary.

The Supplier uses a formal process to capture and approve requirements for any system acquisition or development. This includes the security requirements.

Where applications are accessed on public networks the sensitivity of the data involved informs decisions on the application of controls such as mutual authentication and encryption.

Describe any extra, or changed, controls for this contract.

3.10.2 Security in Development and Support

It is expected that the following words would apply to most organisations but modify as necessary.

Secure development is supported by a Technical Specification document which gives the detailed technical solution that will be developed to deliver the development in question. The purpose of this document is to give detailed and replicable content for the building and review of the proposed solution. The document template includes significant security content and will ensure that security is built into the solution from the earliest stage.

Describe your applicable change control procedures from a security perspective, the testing regime for change, the security applied to the development environment etc.

Describe any extra, or changed, controls for this contract.

3.10.3 Test Data

It is expected that the following words would apply to most organisations but modify as necessary.

Test data is selected to have the least level of value, while still being viable, and may be created specifically for test purposes (for example, where personally identifiable information (PII) is required).

Describe any extra, or changed, controls for this contract.

3.11 Supplier Relationships

3.11.1 Information Security in Supplier Relationships

It is expected that the following words would apply to most organisations but modify as necessary.

All individuals contracted to work as sub-contractors are employed using approved recruitment agencies or on-boarding processes. Contracts of employment for contractors and third parties include non-disclosure and confidentiality terms. Sub-contractors are risk-assessed and, subject to the complexity and scale of any projects they may be required to work on, engagement specific training will be provided to ensure compliance with the Security Policies and SMP.

Other sub-contractors, usually small and medium enterprises or above, are selected with their ability to conform to these security policies in mind, as well as the quality of services that they can offer, and any formal contractual security requirements will be disseminated through their contracts with the Supplier for the provision of the specific services.

All relevant security requirements in the contract are flowed down to sub-contractors.

Describe how these controls apply in this specific contract.

3.11.2 Supplier Service Delivery Management

It is expected that the following words would apply to most organisations but modify as necessary.

Monitoring and review of supplier service delivery is the responsibility of the contracting department within the Supplier. However, it is incumbent on them to involve the security team to ensure that the information security provisions of the agreement are being adhered to and that security incidents are managed properly.

Any service changes will be reviewed by the owner of the supplier relationship, to ensure they meet requirements and any new risks, including information security risks, assessed and dealt with/mitigated as required.

Describe any extra, or changed, controls for this contract.

3.12 Information Security Incident Management

Describe your security incident reporting policy and processes including how it caters for suspected weaknesses in addition to actual incidents. Describe such matters as security triaging, forensic factors, lessons learned etc.

Describe how these controls apply in this specific contract.

Describe any extra, or changed, controls for this contract.

3.13 Business Continuity Management

3.13.1 Information Security Continuity

It is expected that the following words would apply to most organisations but modify as necessary.

The Supplier's business continuity (BC)/disaster recovery (DR) plans cater for the requirement for continuity of information security during incidents, crises or disasters. To achieve this the information security team are a stakeholder in the BC/DR plans. As far as is practicable, information security resilience and recovery are tested during BC/DR exercises.

Describe how BC/DR applies to this contract including how, if necessary, it will fit in with the Buyers BC/DR plans and processes.

3.13.2 Redundancies

Describe your standard redundancy mechanisms and how these will be assessed for whether they meet the requirements of this contract. If they do not, then describe any extra or changed redundancy mechanisms.

3.14 Compliance

3.14.1 Compliance with Legal and Contractual Requirements

It is expected that the following words would apply to most organisations but modify as necessary.

All legal, regulatory and contractual requirements have been identified and are documented in the *{insert document title}.*

The Supplier has an Intellectual Property Rights (IPR) Policy to embed its responsibility to ensure that staff and business processes recognise and act in accordance with legislation governing IPR and the use of proprietary software.

The Supplier operates controls to ensure that records are retained according to the legal requirements.

The Supplier has a policy on data protection for PII in conformance with the Data Protection Act 2018. Privacy is a key part of staff awareness training.

Where cryptographic controls are implemented, the environment in which they are used shall be assessed to ensure relevant parties are aware of all legislation and regulations that relate to that environment.

Describe any extra, or changed, controls for this contract.

3.14.2 Information Security Reviews

The Supplier is formally certified to ISO 27001 (the international standard for information security management). The scope of the certificate (Certificate No: IS 636555) applies to the ISMS relating to the Supplier's common processes used to handle, process and store a client's confidential information, including Protectively Marked Material, in order for the Supplier to carry out client engagements.

The Supplier is subject to six monthly independent surveillance visits by our auditors and is scheduled to undergo a complete re-inspection in Q4 2019.

4 Document Sign-Off

The following people have been assigned with sign-off responsibility for this document:

Responsibility	Name	Sign-off Date
Supplier Security representative	*XXXXXXXX*	*[insert date]*
Other sign off as required	*XXXXXXXX*	*[insert date]*
Other sign off as required	*XXXXXXXX*	*[insert date]*
Buyer Security representative	*XXXXXXXX*	*[insert date]*

Schedule 2: Call-Off Contract charges

[REDACTED]

[REDACTED]

Schedule 3: Collaboration agreement

Not used

Schedule 4: Alternative clauses

Not used

.

Schedule 5: Guarantee

Not used

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 up-todate 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.

Duration of the Processing	From the Start of the Call-Off Contract and for a period of 6 months following the expiry of the Call-Off Contract
Nature and purposes of the Processing	The email address and phone number of users of CVP and VHS. These details are obtained connect users participating in video hearings and video conferences to these functions.
Type of Personal Data	The intention is to only capture the username and phone numbers of users and to track their journey through our digital services. All other personal data, including sensitive data fields, must be masked and protected from unauthorised access. There is no justification or valid reason to view this information.

Categories of Data Subject	Users of the video hearing service which will include private individuals, legal representatives, members of the public observing video hearings, and the Buyers employees
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All Personal Data to be deleted within 6 months of this being collected unless longer retention is required by Law

Annex 2: Joint Controller Agreement

Not used