



## G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:  
G-Cloud 14 Call-Off Contract

### Contents

Schedule 1: Services .....	39
Schedule 2: Call-Off Contract charges .....	41
Schedule 3: Collaboration agreement .....	42
Schedule 4: Alternative clauses .....	43
Schedule 5: Guarantee .....	47
Schedule 6: Glossary and interpretations .....	48
Schedule 7: UK GDPR Information .....	64
Annex 1 - Processing Personal Data .....	64
Exhibit 1 to Schedule 7 .....	68
Schedule 8 (Corporate Resolution Planning) .....	97
Schedule 9 - Variation Form .....	108

## 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.

<b>Platform service ID number</b>	653334924913196
<b>Call-Off Contract reference</b>	C8809
<b>Call-Off Contract title</b>	Service Management Community Training Licenses
<b>Call-Off Contract description</b>	Provision of access to an online Learning Experience Platform (LEP) designed to support the capability development of [REDACTED] within the Service Management Practice.
<b>Start date</b>	24/01/2026
<b>Expiry date</b>	23/01/2029
<b>Call-Off Contract value</b>	<p>The Charges for the Initial Term of 36 months total £386,802 excluding VAT, payable in three annual instalments of £128,934 excluding VAT each.</p> <p>Internal governance approval will be sought for each annual payment before commitment.</p>

	<p>If the Buyer exercises the option to extend the Term by up to 12 months, the additional Charges of £155,000 excluding VAT (inclusive of up to 20% headroom for additional licences if required) will also be subject to separate internal governance approval prior to the extension taking effect.</p> <p>For the avoidance of doubt, the maximum potential value of this Call-Off Contract, inclusive of the optional extension, is £541,802 excluding VAT</p>
<p><b>Charging method</b></p>	<p>Charges will be invoiced electronically by the Supplier and paid by the Buyer via BACS transfer, in accordance with the payment terms set out in this Call-Off Contract</p>
<p><b>Purchase order number</b></p>	<p>To be supplied by the Buyer to the Supplier on contract signature</p>

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14). 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.

<p><b>From the Buyer</b></p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p><b>To the Supplier</b></p>	<p>Skillsoft U.K. Limited</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

**Together the 'Parties'**

**Principal contact details:**

**For the Buyer:**

[Redacted]

**For the Supplier:**

[Redacted]

**Call-Off Contract term**

<b>Start date</b>	This Call-Off Contract Starts on 24/01/2026 and is valid for 36 months.
-------------------	---

<p><b>Ending (termination)</b></p>	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is at least 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>
<p><b>Extension period</b></p>	<p>The Buyer may extend this Call-Off Contract for one additional period of up to 12 months, with an associated value of £155,000 excluding VAT, by providing the Supplier with at least four (4) weeks' written notice prior to the Contract's expiry. This extension is subject to clauses 1.3 and 1.4 in Part B.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>

**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.

<p><b>G-Cloud Lot</b></p>	<p>This Call-Off Contract is for the provision of Services Under:  Lot 2: Cloud software</p>
<p><b>G-Cloud Services required</b></p>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:  Cloud Software</p>
<p><b>Additional Services</b></p>	<p>Not used</p>
<p><b>Location</b></p>	<p>The Services will be delivered remotely.</p>
<p><b>Quality Standards</b></p>	<p>The quality standards required for this Call-Off Contract are:</p> <p><b>Certifications and Frameworks</b></p> <ul style="list-style-type: none"> <li>• ISO/IEC 27001 – Information Security Management.</li> <li>• Cyber Essentials Plus certification.</li> </ul> <p><b>Service Performance</b></p> <ul style="list-style-type: none"> <li>• Ensure system performance meets published specifications and supports concurrent usage as stated in the Service Description.</li> </ul> <p><b>Accessibility and Usability</b></p> <p>The Supplier must comply with Web Content Accessibility Guidelines (WCAG) 2.1 AA accessibility standards at all times during the contract. The Supplier shall achieve WCAG 2.2 AA compliance no later than the end of Year 1 of the contract.</p> <p><b>Data Protection and Compliance</b></p> <ul style="list-style-type: none"> <li>• Full adherence to UK GDPR and the Data Protection Act 2018, including secure data handling and storage within agreed geographic boundaries.</li> </ul> <p><b>Audit and Reporting</b></p> <ul style="list-style-type: none"> <li>• Provide evidence of compliance with the above standards upon request by the Buyer.</li> </ul>

	<ul style="list-style-type: none"> <li>• Notify the Buyer promptly of any material non-compliance and remedial actions.</li> </ul>
<p><b>Technical Standards:</b></p>	<p>The technical standards used as a requirement for this Call-Off Contract are:</p> <p><b>Performance</b></p> <ul style="list-style-type: none"> <li>• Service must operate within the performance parameters stated in the supplier’s Service Definition.</li> </ul> <p><b>Security &amp; Data Protection</b></p> <ul style="list-style-type: none"> <li>• Compliance with UK Government Cloud Security Principles.</li> </ul>
<p><b>Service level agreement:</b></p>	<p>The Service Levels applicable to this Call-Off Contract are those set out in the Supplier’s published G-Cloud Service Definition for Service ID 653334924913196, specifically <b>Exhibit A: “Skillsoft UK Limited – Service Levels &amp; Support”</b>,</p> <p>These Service Levels include:</p> <ul style="list-style-type: none"> <li>• Monthly availability commitment (≥99.5% uptime);</li> <li>• Definition of Downtime and Scheduled Maintenance;</li> <li>• Incident response and resolution times;</li> <li>• Financial recompense model for failure to meet Service Levels;</li> <li>• Technical support and escalation processes.</li> </ul> <p>For the avoidance of doubt, Exhibit A forms part of this Call-Off Contract and shall govern all service performance obligations and remedies.</p>
<p><b>Onboarding</b></p>	<p>The onboarding plan for this Call-Off Contract is not required.</p>

<p><b>Offboarding</b></p>	<p>If the Buyer exercises the option to extend the Term beyond 36 months, the Supplier shall provide an additional exit plan in accordance with clauses 21.3 to 21.8 of the G-Cloud 14 Call-Off Contract Terms.</p>
<p><b>Collaboration agreement</b></p>	<p>Not used.</p>
<p><b>Limit on Parties' liability</b></p>	<p>Defaults by either party resulting in direct loss or damage to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £161,167.50 excluding VAT per year.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater than 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>

<b>Buyer's responsibilities</b>	Not Used
<b>Buyer's equipment</b>	Not Used

Supplier's information

<b>Subcontractors or partners</b>	Not Used
-----------------------------------	----------

Call-Off Contract charges and payment

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

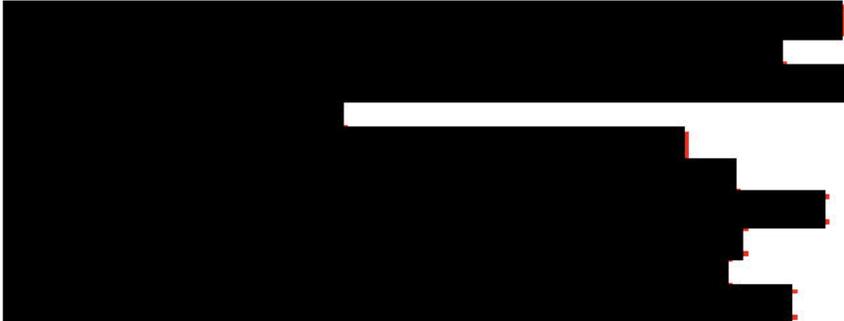
<b>Payment method</b>	The payment method for this Call-Off Contract is <b>BACS</b>
-----------------------	--

<b>Payment profile</b>	The payment profile for this Call-Off Contract is Annually in advance.
<b>Invoice details</b>	The Supplier will issue electronic invoices annually in advance for the software licences as described in Schedule 1: Services. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
<b>Who and where to send invoices to</b>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<b>Invoice information required</b>	<p>[REDACTED]</p> <ul style="list-style-type: none"><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li></ul>

	<p>Multiple invoices can be attached to one email but each invoice must be in a separate PDF (with no additional supporting files as described above).</p>
<b>Invoice frequency</b>	<p>Invoice will be sent to the Buyer annually in advance.</p>
<b>Call-Off Contract value</b>	<p>The Charges for the Initial Term of 36 months total £386,802 excluding VAT, payable in three annual instalments of £128,934 excluding VAT each.</p> <p>Internal governance approval will be sought for each annual payment before commitment.</p> <p>If the Buyer exercises the option to extend the Term by up to 12 months, the additional Charges of £155,000 excluding VAT (inclusive of up to 20% headroom for additional licences if required) will also be subject to separate internal governance approval prior to the extension taking effect.</p> <p>For the avoidance of doubt, the maximum potential value of this Call-Off Contract, inclusive of the optional extension, is £541,802 excluding VAT</p>
<b>Call-Off Contract charges</b>	<p>See Schedule 2: Pricing</p>

### Additional Buyer terms

<p><b>Performance of the Service</b></p>	<p>See Schedule 1: Services</p>
<p><b>Guarantee</b></p>	<p>Not used</p>
<p><b>Warranties, representations</b></p>	<p>Not used</p>
<p><b>Supplemental requirements in addition to the Call-Off terms</b></p>	<p>Not used</p>
<p><b>Alternative clauses</b></p>	<p>Not used</p>

<b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b>	The Supplier shall attend monthly review meetings with the Buyer to discuss service performance, usage, and any issues arising under this Call-Off Contract. Meetings will be scheduled by mutual agreement and may be conducted virtually. Additional meetings may be convened by the Buyer on reasonable notice if required to address urgent matters
<b>Personal Data and Data Subjects</b>	See Schedule 7 Annex 3    





	
<p><b>Intellectual Property</b></p>	<p>No Buyer-specific Intellectual Property Rights (IPR) requirements apply under this Call-Off Contract. Intellectual Property Rights shall be governed by the Supplier’s published G-Cloud Terms and Conditions associated with Service ID 653334924913196, as incorporated into this Call-Off Contract.</p> <p>The Buyer receives only the non-exclusive, non-transferable license granted for internal training purposes during the Contract Term. Any modifications or updates to Supplier products shall not be deemed Project Specific IPR</p>
<p><b>Social Value</b></p>	<p>Are those set out in the Supplier’s published G-Cloud Service Definition for Service ID 653334924913196</p>
<p><b>Performance Indicators</b></p>	<p>Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.</p> <p>Buyer may from time to time request information relating to Supplier’s performance of service levels and support as described in the Supplier’s published G-Cloud Service Definition for Service ID 653334924913196.</p> <p>Any other Performance Indicators will be agreed between the Parties on an ad hoc basis.</p> <p>Supplier shall provide quarterly reports on service performance and attend quarterly review meetings with the Buyer to discuss these indicators and any remedial actions.</p>

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 clauses 8.3 to 8.6 inclusive 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 RM1557.14.

<b>Signed</b>	Supplier	Buyer
<b>Name</b>	[REDACTED]	[REDACTED]
<b>Title</b>	[REDACTED]	[REDACTED]
<b>Signature</b>	[REDACTED]	[REDACTED]
<b>Date</b>	1/20/2026	1/21/2026

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

## Buyer Benefits

For each Call-Off Contract please complete a buyer benefits record, by following this link:  
[G-Cloud 14 Customer Benefit Record](#)

### Part B: Terms and conditions

1. Call-Off Contract Start date and length
  - 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
  - 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
  - 1.3 The 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 36 months.

### 2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules 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)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (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)
- 30 (Insurance)
- 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
- 2.2.4 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.
- 2.2.5 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.
- 2.2.6 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 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

### 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

### 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

## 5. Due diligence

### 5.1 Both Parties agree that when entering into a Call-Off Contract they:

- 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.

## 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 employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
- 9.4.1 a broker's verification of insurance
  - 9.4.2 receipts for the insurance premium
  - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
- 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
  - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
  - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

## 10. Confidentiality

- 10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11. Intellectual Property Rights

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

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

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

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

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

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

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

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

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

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

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

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

11.8 Clause 11.6 will not apply if the IPR Claim is from:  
the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract  
other material provided by the Buyer necessary for the Services

11.9 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-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.npsa.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets:

<https://www.npsa.gov.uk/sensitive-information-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/technologycode-of-practice/technology-code-of-practice>

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

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

## 15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

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

## 16. Security

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

## 17. Guarantee

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

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

## 18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.
- 18.2 The Parties agree that the:
  - 18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
  - 18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses
- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
  - 18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
  - 18.4.2 any fraud
- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
  - 18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
  - 18.5.2 an Insolvency Event of the other Party happens
  - 18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business
- 18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the

Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this 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:

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

plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO 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 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.
- 23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.
- 23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

## 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

24.5 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 is not a 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 cooperate 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 using the template in Schedule 9 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 using the template in Schedule 9. 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

### **Background & Context**

The Service Management Practice supports the capability and development of approximately 1,200 members. Central to this is access to an online Learning Experience Platform (LXP) that provides multi-channel learning (videos, tutorials, books, etc.) on Service Management.

This LXP is a major enabler of the Service Management Practice Development Offering and aims to increase the capability and professionalism of the Practice and its members.

### **Buyer Specification (DWP Requirements)**

The Buyer requires:

- An online, 24/7 blended learning platform providing multi-channel delivery (video, audio, books, labs) accessible across multiple devices.
- Coverage of all aspects of Service Management
- Alignment with the Government Digital and Data Profession Capability (GDAD) Framework.
- Clear output-based deliverables with acceptance criteria to ensure accountability for delivery.
- Learning in the Digital/Technology field
- Guided learning and structured learning paths aligned to DDaT/GDAD frameworks.
- Multi-channel delivery across multiple devices.
- Minimum compliance with WCAG 2.1 AA accessibility standards.
- Inclusive Learning Design: The platform should reduce barriers to learning, including mobile access, flexible formats, and support for diverse learning needs.

The Supplier will provide 'Service Management Community Training Licenses' as described in the G-Cloud Service Offering, service ID: 653334924913196. The Supplier's Service Definition and Terms & Conditions published on the CCS Digital Marketplace on 08/10/2025 shall apply and are incorporated into this Call-Off (embedded below). Any subsequent updates shall not apply unless agreed in writing by both Parties. In the event of any conflict or ambiguity, the terms of this Call-Off Contract (including this Schedule and the Order Form) shall take precedence over the Supplier's published terms, in accordance with clauses 8.3 to 8.6 of the Framework Agreement.

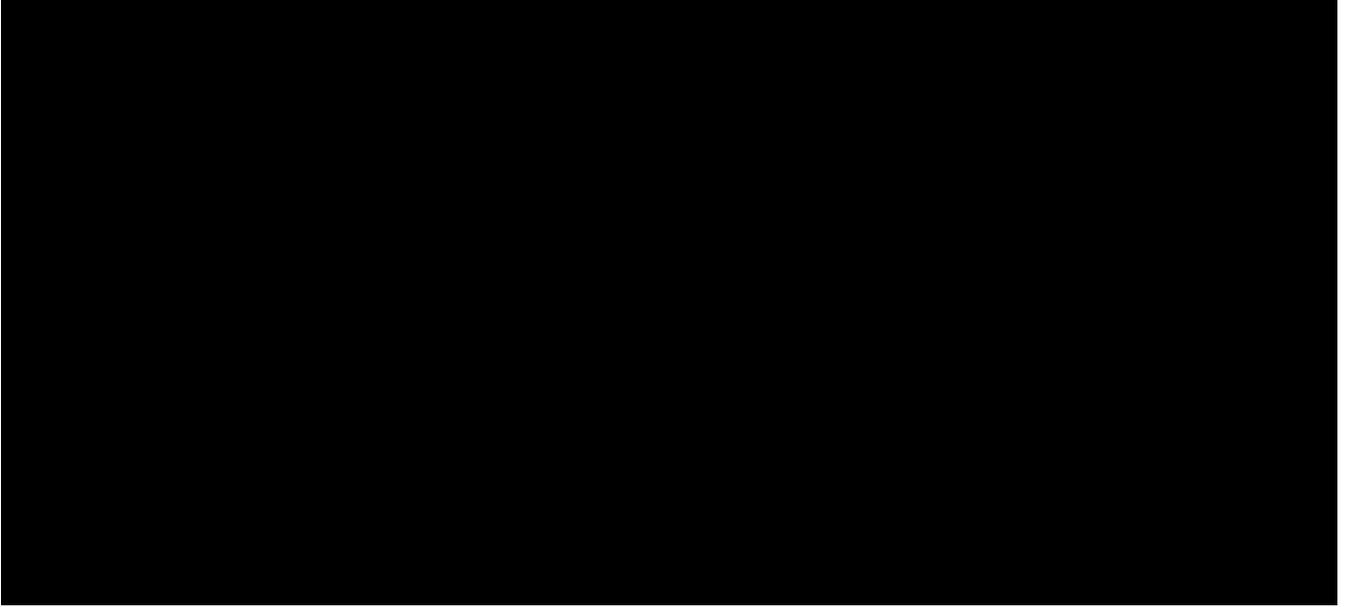


service-definition-d  
ocument-version da



terms-and-conditio  
ns-version dated 08.

## Schedule 2: Call-Off Contract charges



Internal governance approval will be sought for each annual payment before commitment.

## Schedule 3: Collaboration agreement

Not Used

## Schedule 4: Alternative clauses

### 1. Introduction

- 1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

### 2. Clauses selected

- 2.1 The Buyer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

- 2.2 The Buyer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

### 2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

Employment (Northern Ireland) Order 2002

Fair Employment and Treatment (Northern Ireland) Order 1998

Sex Discrimination (Northern Ireland) Order 1976 and 1988

Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003

Equal Pay Act (Northern Ireland) 1970

Disability Discrimination Act 1995

Race Relations (Northern Ireland) Order 1997

Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996  
Employment Equality (Age) Regulations (Northern Ireland) 2006  
Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000  
Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002  
The Disability Discrimination (Northern Ireland) Order 2006  
The Employment Relations (Northern Ireland) Order 2004  
Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006  
Employment Relations (Northern Ireland) Order 2004  
Work and Families (Northern Ireland) Order 2006

and will use its best endeavours to ensure that in its employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract it promotes equality of treatment and opportunity between:

persons of different religious beliefs or political opinions  
men and women or married and unmarried persons  
persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)  
persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)  
persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)  
persons of different ages  
persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

## 2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Buyer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

the issue of written instructions to staff and other relevant persons  
the appointment or designation of a senior manager with responsibility for equal opportunities  
training of all staff and other relevant persons in equal opportunities and harassment matters  
the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Buyer as soon as possible in the event of: the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Term by any Industrial or Fair Employment Tribunal or court, The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Buyer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Buyer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Buyer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

## 2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Buyer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Buyer in relation to same.

## 2.6 Health and safety

2.6.1 The Supplier will promptly notify the Buyer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Buyer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Buyer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Buyer premises, the Supplier will comply with any health and safety measures implemented by the Buyer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Buyer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Buyer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Buyer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Buyer on request.

## 2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).

2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

## Schedule 5: Guarantee

Not Used

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

<b>Expression</b>	<b>Meaning</b>
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses.
<b>Background IPRs</b>	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.
<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.

<p><b>Buyer Software</b></p>	<p>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.</p>
<p><b>Call-Off Contract</b></p>	<p>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.</p>
<p><b>Charges</b></p>	<p>The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.</p>
<p><b>Collaboration Agreement</b></p>	<p>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.</p>
<p><b>Commercially Sensitive Information</b></p>	<p>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.</p>

<p><b>Confidential Information</b></p>	<p>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').</p>
<p><b>Control</b></p>	<p>'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.</p>
<p><b>Controller</b></p>	<p>Takes the meaning given in the UK GDPR.</p>
<p><b>Crown</b></p>	<p>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.</p>
<p><b>Data Loss Event</b></p>	<p>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.</p>
<p><b>Data Protection Impact Assessment (DPIA)</b></p>	<p>An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.</p>

<b>Data Protection Legislation (DPL)</b>	(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.
<b>Data Subject</b>	Takes the meaning given in the UK GDPR
<b>Default</b>	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.
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: <a href="https://www.gov.uk/guidance/check-employment-status-fortax">https://www.gov.uk/guidance/check-employment-status-fortax</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.
<b>Financial Metrics</b>	The following financial and accounting measures: Dun and Bradstreet score of 50 Operating Profit Margin of 2% Net Worth of 0 Quick Ratio of 0.7

<p><b>Force Majeure</b></p>	<p>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</p>
<p><b>Former Supplier</b></p>	<p>A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).</p>
<p><b>Framework Agreement</b></p>	<p>The clauses of framework agreement RM1557.14 together with the Framework Schedules.</p>

<b>Fraud</b>	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
<b>Freedom of Information Act or FoIA</b>	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement 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.
<b>UK GDPR</b>	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.

<b>Implementation Plan</b>	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.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.

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

<b>Insolvency event</b>	Can be: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium a Supplier Trigger Event
<b>Intellectual Property Rights or IPR</b>	Intellectual Property Rights are: (a) 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 (b) 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 (c) all other rights having equivalent or similar effect in any country or jurisdiction

<b>Intermediary</b>	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).
<b>IPR claim</b>	As set out in clause 11.5.
<b>IR35</b>	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
<b>IR35 assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
<b>Law</b>	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, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement Schedule 6.
<b>Material Breach</b>	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

<b>New Fair Deal</b>	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
<b>Order</b>	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.

<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
<b>Performance Indicators</b>	The performance information required by the Buyer from the Supplier set out in the Order Form.
<b>Personal Data</b>	Takes the meaning given in the UK GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the UK GDPR.
<b>Platform</b>	The government marketplace where Services are available for Buyers to buy.
<b>Processing</b>	Takes the meaning given in the UK GDPR.
<b>Processor</b>	Takes the meaning given in the UK GDPR.

<p><b>Prohibited act</b></p>	<p>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</p>
------------------------------	---

<p><b>Project Specific IPRs</b></p>	<p>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.</p>
<p><b>Property</b></p>	<p>Assets and property including technical infrastructure, IPRs and equipment.</p>
<p><b>Protective Measures</b></p>	<p>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.</p>

<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.
<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
<b>Replacement supplier</b>	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.

<b>Service Data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.
<b>Service definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
<b>Service description</b>	The description of the Supplier service offering as published on the Platform.
<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controlsche-ck-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controlsche-ck-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
<b>Subcontractor</b>	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off

	Contract) and its servants or agents in connection with the provision of G-Cloud Services.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

<b>Supplier staff</b>	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
<b>Supplier Terms</b>	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.
<b>Trigger Event</b>	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).

<p><b>Variation Impact Assessment</b></p>	<p>An assessment of the impact of a variation request by the Buyer completed in good faith, including:          details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract;          details of the cost of implementing the proposed variation;          details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;          a timetable for the implementation, together with any proposals for the testing of the variation; and          such other information as the Buyer may reasonably request in (or in response to) the variation request;</p>
<p><b>Working Days</b></p>	<p>Any day other than a Saturday, Sunday or public holiday in England and Wales.</p>
<p><b>Year</b></p>	<p>A contract year.</p>

## 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 Alexis Hernandez  
[REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p><b>The Buyer is Controller and the Supplier is Processor</b>                      The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>To create and manage user accounts for Buyer's employees on the Supplier's learning platform. To enable access to learning content and track progress for reporting purposes. Types of personal data include:</p> <p>Name, e-mail address, job role and organisational position.</p> <p><b>The Parties are Independent Controllers of Personal Data</b></p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:                      Business contact details of Supplier Personnel for which the Supplier is the Controller,</i></p>





	
Categories of Data Subject	Employees of the Buyer who will access the learning platform. Business contacts of the Buyer and Supplier (for contract management purposes).
International transfers and legal gateway	No international transfers of personal data will take place.

<p>Plan for return and destruction of the data once the Processing is complete</p>	<p>Upon termination or expiry of the Call-Off Contract, the Supplier shall, within 30 days, securely delete or return all personal data processed on behalf of the Buyer, unless retention is required by law or otherwise agreed in writing.</p>
--	---

## Exhibit 1 to Schedule 7



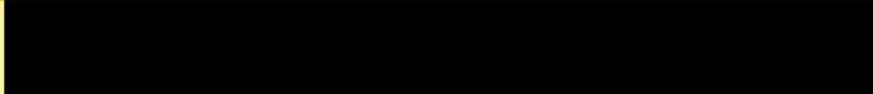
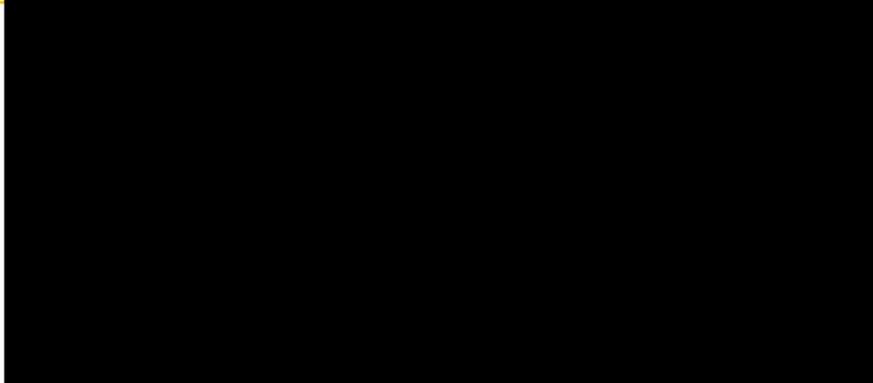
Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1)  
 Data Protection Act 2018  
 International Data Transfer Agreement  
 VERSION A1.0, in force 21 March 2022

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties and signatures

<p>Start date</p>	<p>17/20/2020</p>
<p>The Parties</p>	
<p>Parties' details</p>	

Key Contact	
Importer Data Subject Contact	
Signatures confirming each Party agrees to be bound by this IDTA	

Table 2: Transfe

UK country's law that governs the IDTA:	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
Primary place for legal claims to be made by the Parties	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller

	<p><input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor  <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)</p>
<p>Whether UK GDPR applies to the Importer</p>	<p><input checked="" type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data  <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data</p>
<p>Linked Agreement</p>	<p>If the Importer is the Exporter's Processor or Sub-Processor – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:  Name of agreement: G-Cloud 14 Call-Off Contract  Parties to the agreement: DWP  Reference (if any): _____</p> <p>Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:  Name of agreement: none  Date of agreement: n.a.  Parties to the agreement: n.a.  Reference (if any):</p> <p>If the Exporter is a Processor or Sub-Processor – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:  Name of agreement:  Date of agreement:  Parties to the agreement:  Reference (if any):</p>
<p>Term</p>	<p>The Importer may Process the Transferred Data for the following time period:  <input checked="" type="checkbox"/> the period for which the Linked Agreement is in force  <input type="checkbox"/> time period:  <input type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.</p>

<p>Ending the IDTA before the end of the Term</p>	<p><input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.</p> <p><input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving:</p> <p>    <input type="checkbox"/> months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).</p>
<p>Ending the IDTA when the Approved IDTA changes</p>	<p>Which Parties may end the IDTA as set out in Section 29.2:</p> <p><input type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input checked="" type="checkbox"/> neither Party</p>
<p>Can the Importer make further transfers of the Transferred Data?</p>	<p><input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p> <p><input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p>
<p>Specific restrictions when the Importer may transfer on the Transferred Data</p>	<p>The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:</p> <p><input type="checkbox"/> if the Exporter tells it in writing that it may do so.</p> <p><input type="checkbox"/> to:</p> <p><input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in:</p> <p><input checked="" type="checkbox"/> there are no specific restrictions.</p>
<p>Review Dates</p>	<p><input type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data</p> <p>First review date:</p> <p>The Parties must review the Security Requirements at least once:</p> <p><input type="checkbox"/> each <input type="checkbox"/> month(s)</p> <p><input type="checkbox"/> each quarter</p> <p><input type="checkbox"/> each 6 months</p> <p><input type="checkbox"/> each year</p> <p><input type="checkbox"/> each <input type="checkbox"/> year(s)</p> <p><input checked="" type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment</p>

Table 3: Transferred Data

<p>Transferred Data</p>	<p>The personal data to be sent to the Importer under this IDTA consists of: First Name, Last Name, Display First Name, Display Last Name, Company Email Address, Office Location, Login Name, Password, User ID, Username, other non-sensitive data relating to the individual's place in the Exporter's organisation, and learning accessed by the individual.</p> <p><input checked="" type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
<p>Special Categories of Personal Data and criminal convictions and offences</p>	<p>The Transferred Data includes data relating to:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> racial or ethnic origin</li> <li><input type="checkbox"/> political opinions</li> <li><input type="checkbox"/> religious or philosophical beliefs</li> <li><input type="checkbox"/> trade union membership</li> <li><input type="checkbox"/> genetic data</li> <li><input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person</li> <li><input type="checkbox"/> physical or mental health</li> <li><input type="checkbox"/> sex life or sexual orientation</li> <li><input type="checkbox"/> criminal convictions and offences</li> <li><input checked="" type="checkbox"/> none of the above</li> <li><input type="checkbox"/> set out in:</li> </ul> <p>And:</p> <p><input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
<p>Relevant Data Subjects</p>	<p>The Data Subjects of the Transferred Data are: staff of Importer</p> <p><input checked="" type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>

Purpose	<p><input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes:</p> <p><input checked="" type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in: the Linked Agreement (G-Cloud 15 Call-Off Contract)</p> <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> <p><input checked="" type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
---------	--

Table 4: Security Requirements

Security of Transmission	Refer to the Supplier's document titled Percipio Security and Infrastructure Overview for US and EU Deployment Locations appended as Annex 1 to Supplier's G-Cloud 15 Service Definition Document available at the Digital Marketplace and also available at <a href="https://documentation.skillssoft.com/">https://documentation.skillssoft.com/</a>
Security of Storage	Refer to the Supplier's document titled Percipio Security and Infrastructure Overview for US and EU Deployment Locations appended as Annex 1 to Supplier's G-Cloud 15 Service Definition Document available at the Digital Marketplace and also available at <a href="https://documentation.skillssoft.com/">https://documentation.skillssoft.com/</a>
Security of Processing	Refer to the Supplier's document titled Percipio Security and Infrastructure Overview for US and EU Deployment Locations appended as Annex 1 to Supplier's G-Cloud 15 Service Definition Document available at the Digital Marketplace and also available at <a href="https://documentation.skillssoft.com/">https://documentation.skillssoft.com/</a>
Organisational security measures	Refer to the Supplier's document titled Percipio Security and Infrastructure Overview for US and EU Deployment Locations appended as Annex 1 to Supplier's G-Cloud 15 Service Definition Document available at the Digital Marketplace and also available at <a href="https://documentation.skillssoft.com/">https://documentation.skillssoft.com/</a>
Technical security minimum requirements	Refer to the Supplier's document titled Percipio Security and Infrastructure Overview for US and EU Deployment Locations appended as Annex 1 to Supplier's G-Cloud 15 Service Definition Document available at the Digital Marketplace and also available at <a href="https://documentation.skillssoft.com/">https://documentation.skillssoft.com/</a>

Updates to the Security Requirements	<input checked="" type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
--------------------------------------	--

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

Part 3: Commercial Clauses

Commercial Clauses	Contained in the Linked Agreement.
--------------------	------------------------------------

Part 4: Mandatory Clauses

XX

## Information that helps you to understand this IDTA

- 1. This IDTA and Linked Agreements**
  - 1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
  - 1.2 This IDTA is made up of:
    - 1.2.1 Part one: Tables;
    - 1.2.2 Part two: Extra Protection Clauses;
    - 1.2.3 Part three: Commercial Clauses; and
    - 1.2.4 Part four: Mandatory Clauses.
  - 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
  - 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
  - 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.
- 2. Legal Meaning of Words**
  - 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
  - 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.
- 3. You have provided all the information required**
  - 3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
  - 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
    - 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
    - 3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
  - 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.
- 4. How to sign the IDTA**
  - 4.1 The Parties may choose to each sign (or execute):
    - 4.1.1 the same copy of this IDTA;

- 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
- 4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

**5. Changing this IDTA**

- 5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:
  - 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
  - 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
  - 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
  - 5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4; provided that the changes do not reduce the Appropriate Safeguards.
- 5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.4 From time to time, the ICO may publish a revised Approved IDTA which:

- 5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or
- 5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

**6. Understanding this IDTA**

- 6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
- 6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.
- 6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.
- 6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.
- 6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.
- 6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.
- 6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):
  - 6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and
  - 6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.
- 6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.
- 6.9 References to:
  - 6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;
  - 6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that

- 6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

**7. Which laws apply to this IDTA**

- 7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

**How this IDTA provides Appropriate Safeguards**

**8. The Appropriate Safeguards**

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
  - 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
  - 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter must:
  - 8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
  - 8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.
- 8.3 The Importer must:
  - 8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");
  - 8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;
  - 8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
  - 8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.
- 8.4 The Importer must ensure that at the Start Date and during the Term:
  - 8.4.1 the Importer Information is accurate;

- 8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.
- 8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
- 9. Reviews to ensure the Appropriate Safeguards continue**
- 9.1 Each Party must:
  - 9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and
  - 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
  - 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;
  - 9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and
  - 9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.
- 10. The ICO**
- 10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
- 10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
- 10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.
- The Exporter**
- 11. Exporter's obligations**
- 11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
- 11.2 The Exporter must:

- 11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
- 11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
- 11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.
- 11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.
- 11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.
- 11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

**The Importer**

**12. General Importer obligations**

- 12.1 The Importer must:
  - 12.1.1 only Process the Transferred Data for the Purpose;
  - 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
  - 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
  - 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
  - 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
  - 12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).
- 12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

**13. Importer's obligations if it is subject to the UK Data Protection Laws**

- 13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

- 13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and
- 13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.
- 13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:
  - Section 14 (Importer’s obligations to comply with key data protection principles);
  - Section 15 (What happens if there is an Importer Personal Data Breach);
  - Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
  - Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter’s Processor or Sub-Processor).
- 14. Importer’s obligations to comply with key data protection principles**
- 14.1 The Importer does not need to comply with this Section 14 if it is the Exporter’s Processor or Sub-Processor.
- 14.2 The Importer must:
  - 14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;
  - 14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and
  - 14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.
- 15. What happens if there is an Importer Personal Data Breach**
- 15.1 If there is an Importer Personal Data Breach, the Importer must:
  - 15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter’s Processor or Sub-Processor: these steps must comply with the Exporter’s instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and
  - 15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
- 15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:
  - 15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

- 15.2.1.1 a description of the nature of the Importer Personal Data Breach;
- 15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
- 15.2.1.3 likely consequences of the Importer Personal Data Breach;
- 15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
- 15.2.1.5 contact point for more information; and
- 15.2.1.6 any other information reasonably requested by the Exporter,
- 15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and
- 15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.
- 15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
  - 15.3.1 a description of the nature of the Importer Personal Data Breach;
  - 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
  - 15.3.3 likely consequences of the Importer Personal Data Breach;
  - 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
  - 15.3.5 contact point for more information; and
  - 15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.
- 15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

**16. Transferring on the Transferred Data**

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:
  - 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
  - 16.1.2 the third party has been added to this IDTA as a Party; or
  - 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
  - 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
  - 16.1.5 the transfer is to the UK or an Adequate Country.
- 16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

**17. Importer’s responsibility if it authorises others to perform its obligations**

- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
- 17.2 If the Importer is the Exporter’s Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
- 17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
- 17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

**What rights do individuals have?**

**18. The right to a copy of the IDTA**

- 18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:
  - 18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

- 18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
- 18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

**19. The right to Information about the Importer and its Processing**

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

**20. How Relevant Data Subjects can exercise their data subject rights**

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

- 20.4.1 Without Undue Delay (and in any event within one month);
- 20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;
- 20.4.3 in clear and plain English that is easy to understand; and
- 20.4.4 in an easily accessible form

together with

- 20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
  - 20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
- 20.5 If a Relevant Data Subject requests, the Importer must:
- 20.5.1 rectify inaccurate or incomplete Transferred Data;
  - 20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;
  - 20.5.3 cease using it for direct marketing purposes; and
  - 20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the “Decision-Making”), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
- 20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or
  - 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
  - 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.
- 21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor**
- 21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.
- 22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws**
- 22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
- 22.1.1 it is unable to reasonably verify the identity of an individual making the request; or
  - 22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

- 22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

**How to give third parties access to Transferred Data under Local Laws**

**23. Access requests and direct access**

- 23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.
- 23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.
- 23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.
- 23.4 In so far as Local Laws allow, the Importer must:
  - 23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed;
  - 23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

**24. Giving notice**

- 24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
- 24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.
- 24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

**25. General clauses**

- 25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:
  - 25.1.1 contain all the terms and conditions agreed by the Parties; and
  - 25.1.2 override all previous contacts and arrangements, whether oral or in writing.

- 25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
- 25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
- 25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.
- 25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.
- 25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:
  - 25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;
  - 25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
  - 25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

**What happens if there is a breach of this IDTA?**

- 26. **Breaches of this IDTA**
- 26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:
  - 26.1.1 has breached this IDTA; or
  - 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
- 26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.
- 27. **Breaches of this IDTA by the Importer**
- 27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
  - 27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

- 27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
- 27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:
  - 27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and
  - 27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).
- 27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.
- 28. Breaches of this IDTA by the Exporter**
- 28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.
- 28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

#### **Ending the IDTA**

- 29. How to end this IDTA without there being a breach**
- 29.1 The IDTA will end:
  - 29.1.1 at the end of the Term stated in Table 2: Transfer Details; or
  - 29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;
  - 29.1.3 at any time that the Parties agree in writing that it will end; or
  - 29.1.4 at the time set out in Section 29.2.
- 29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:
  - 29.2.1 its direct costs of performing its obligations under the IDTA; and/or
  - 29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

**30. How to end this IDTA if there is a breach**

- 30.1 A Party may end this IDTA immediately by giving the other Party written notice if:
- 30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and
    - 30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
    - 30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;
  - 30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

**31. What must the Parties do when the IDTA ends?**

- 31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:
- 31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;
  - 31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and
  - 31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.
- 31.2 When this IDTA ends (no matter what the reason is):
- 31.2.1 the Exporter must stop sending Transferred Data to the Importer; and
  - 31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;
  - 31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.
  - 31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):
    - **Section 1** (This IDTA and Linked Agreements);
    - **Section 2** (Legal Meaning of Words);

- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

**How to bring a legal claim under this IDTA**

**32. Your liability**

- 32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.
- 32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:
- 32.2.1 Party One's breach of this IDTA; and/or
  - 32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;
  - 32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

- 32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.
- 32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

**33. How Relevant Data Subjects and the ICO may bring legal claims**

- 33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):
- **Section 1** (This IDTA and Linked Agreements);
  - **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
  - **Section 8** (The Appropriate Safeguards);
  - **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
  - **Section 11** (Exporter's obligations);
  - **Section 12** (General Importer Obligations);
  - **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
  - **Section 14** (Importer's obligations to comply with key data protection laws);
  - **Section 15** (What happens if there is an Importer Personal Data Breach);
  - **Section 16** (Transferring on the Transferred Data);
  - **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
  - **Section 18** (The right to a copy of the IDTA);
  - **Section 19** (The Importer's contact details for the Relevant Data Subjects);
  - **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
  - **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
  - **Section 23** (Access Requests and Direct Access);
  - **Section 26** (Breaches of this IDTA);
  - **Section 27** (Breaches of this IDTA by the Importer);
  - **Section 28** (Breaches of this IDTA by the Exporter);
  - **Section 30** (How to end this IDTA if there is a breach);
  - **Section 31** (What must the Parties do when the IDTA ends); and
  - any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.
- 33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).
- 33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
- 33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.
- 33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

- 34. Courts legal claims can be brought in**
- 34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
- 34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
- 34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).
- 35. Arbitration**
- 35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.
- 35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.
- 35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.
- 35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.
- 35.5 The English language must be used in the arbitral proceedings.
- 35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.
- 36. Legal Glossary**

<b>Word or Phrase</b>	<b>Legal definition (this is how this word or phrase must be interpreted in the IDTA)</b>
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.

<b>Word or Phrase</b>	<b>Legal definition (this is how this word or phrase must be interpreted in the IDTA)</b>
Adequate Country	<p>A third country, or:</p> <ul style="list-style-type: none"> <li>• a territory;</li> <li>• one or more sectors or organisations within a third country;</li> <li>• an international organisation;</li> </ul> <p>which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.</p>
Appropriate Safeguards	<p>The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.</p>
Approved IDTA	<p>The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4.</p>
Commercial Clauses	<p>The commercial clauses set out in Part three.</p>
Controller	<p>As defined in the UK GDPR.</p>
Damage	<p>All material and non-material loss and damage.</p>
Data Subject	<p>As defined in the UK GDPR.</p>
Decision-Making	<p>As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.</p>
Direct Access	<p>As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.</p>
Exporter	<p>The exporter identified in Table 1: Parties &amp; Signature.</p>
Extra Protection Clauses	<p>The clauses set out in Part two: Extra Protection Clauses.</p>
ICO	<p>The Information Commissioner.</p>

<b>Word or Phrase</b>	<b>Legal definition (this is how this word or phrase must be interpreted in the IDTA)</b>
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.

<b>Word or Phrase</b>	<b>Legal definition (this is how this word or phrase must be interpreted in the IDTA)</b>
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards

<b>Word or Phrase</b>	<b>Legal definition (this is how this word or phrase must be interpreted in the IDTA)</b>
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

<b>Mandatory Clauses</b>	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA.A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.
--------------------------	--

## Schedule 8 (Corporate Resolution Planning)

### 1. Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

<b>"Accounting Reference Date"</b>	means in each year the date to which the Supplier prepares its annual audited financial statements;
<b>"Annual Revenue"</b>	means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology: figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
<b>"Appropriate Authority" or "Appropriate Authorities"</b>	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
<b>"Associates"</b>	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
<b>"Cabinet Office Markets and Suppliers Team"</b>	means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
<b>"Class 1 Transaction"</b>	has the meaning set out in the listing rules issued by the UK Listing Authority;

<p><b>“Control”</b></p>	<p>the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;</p>
<p><b>“Corporate Change Event”</b></p>	<p>means:  any change of Control of the Supplier or a Parent Undertaking of the Supplier;  any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;  any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;  a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;  an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;  payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;  an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;  any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;  the appointment of a receiver, administrative receiver or administrator in respect of or over all</p>

	or a material part of the undertaking or assets of any member of the Supplier Group; and/or any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;
<b>"Corporate Change Event Grace Period"</b>	means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;
<b>"Corporate Resolvability Assessment (Structural Review)"</b>	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;
<b>"Critical National Infrastructure" or "CNI"</b>	means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or significant impact on the national security, national defence, or the functioning of the UK;
<b>"Critical Service Contract"</b>	means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;
<b>"CRP Information"</b>	means the corporate resolution planning information, together, the: (a) Exposure Information (Contracts List); (b) Corporate Resolvability Assessment (Structural Review); and (c) Financial Information and Commentary
<b>"Dependent Parent Undertaking"</b>	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance

	<p>of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;</p>
<p><b>“FDE Group”</b>  <b>“Financial Distress Event”</b></p>	<p>means the Supplier and Subcontractors</p> <p>the credit rating of an FDE Group entity dropping below the applicable Financial Metric;  an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;  there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;  an FDE Group entity committing a material breach of covenant to its lenders;  a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;  any of the following:  commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;  non-payment by an FDE Group entity of any financial indebtedness;  any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;  the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity;  or  the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;  in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and</p>

	any two of the Financial Metrics for the Supplier not being met at the same time.
<b>“Parent Undertaking”</b>	has the meaning set out in section 1162 of the Companies Act 2006;
<b>“Public Sector Dependent Supplier”</b>	means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;
<b>“Strategic Supplier”</b>	means those suppliers to government listed at <a href="https://www.gov.uk/government/publications/strategic-suppliers">https://www.gov.uk/government/publications/strategic-suppliers</a> ;
<b>“Subsidiary Undertaking”</b>	has the meaning set out in section 1162 of the Companies Act 2006;
<b>“Supplier Group”</b>	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
<b>“UK Public Sector Business”</b>	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and
<b>“UK Public Sector / CNI Contract Information”</b>	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;

### Service Status and Supplier Status

This Call-Off Contract is not a Critical Service Contract.

The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is [REDACTED]

The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer’s rights under this Schedule.

### Provision of Corporate Resolution Planning Information

Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.

Subject to Paragraphs 3.6, 3.10 and 3.11:

where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and  
except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.

The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

is full, comprehensive, accurate and up to date;  
is split into three parts:  
Exposure Information (Contracts List);  
Corporate Resolvability Assessment (Structural Review);

## Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at <https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and

complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the

CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and

no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.

If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11)

unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;

within 30 days of a Corporate Change Event unless, the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

not required pursuant to Paragraph 3.10;

within 30 days of the date that:

the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or  
none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and  
in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or

not required pursuant to Paragraph 3.10.

Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:  
Aa3 or better from Moody's;  
AA- or better from Standard and Poors;  
AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the

Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

## Termination Rights

The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

## Confidentiality and usage of CRP Information

The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality. Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.

The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

redacting only those parts of the information which are subject to such obligations of confidentiality;

providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:  
summarising the information;  
grouping the information;  
anonymising the information; and  
presenting the information in general terms

The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

## **ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST**

The Supplier shall:

provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:

are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;

are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or

involve or could reasonably be considered to involve CNI;

provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

## **ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)**

The Supplier shall:

provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;

ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and

provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

### ANNEX 3: Financial information AND COMMENTARY

The Supplier shall:

provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and

ensure that the information is presented in a simple, effective and easily understood manner. For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

## Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

<b>Contract Details</b>		
This variation is between:	<b>[insert]</b> name of Buyer] (“the Buyer”) And <b>[insert]</b> name of Supplier] (“the Supplier”)	
Contract name:	<b>[insert]</b> name of contract to be changed] (“the Contract”)	
Contract reference number:	<b>[insert]</b> contract reference number]	
<b>Details of Proposed Variation</b>		
Variation initiated by:	<b>[delete]</b> as applicable: Buyer/Supplier]	
Variation number:	<b>[insert]</b> variation number]	
Date variation is raised:	<b>[insert]</b> date]	
Proposed variation		
Reason for the variation:	<b>[insert]</b> reason]	
A Variation Impact Assessment shall be provided within:	<b>[insert]</b> number] days	
<b>Impact of Variation</b>		
Likely impact of the proposed variation:	<b>[Supplier to insert]</b> assessment of impact]	
<b>Outcome of Variation</b>		
Contract variation:	This Contract detailed above is varied as follows: <b>[Buyer to insert]</b> original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ <b>[insert]</b> amount]
	Additional cost due to variation:	£ <b>[insert]</b> amount]
	New Contract value:	£ <b>[insert]</b> amount]

This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

Words and expressions in this Variation shall have the meanings given to them in the Contract.

The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature \_\_\_\_\_  
Date \_\_\_\_\_  
Name (in Capitals) \_\_\_\_\_  
Address \_\_\_\_\_

---

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature \_\_\_\_\_  
Date \_\_\_\_\_  
Name (in Capitals) \_\_\_\_\_  
Address \_\_\_\_\_