

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE: Ecm_11664

CALL-OFF TITLE: Data Access Layer (DAL) Factory

CALL-OFF CONTRACT DESCRIPTION: Provision of Government Digital and Data Resources for the Data Access Layer (DAL)

THE BUYER: Department for Work and Pensions

BUYER ADDRESS Redacted

THE SUPPLIER: CGI IT UK Limited

SUPPLIER ADDRESS: Redacted

REGISTRATION NUMBER: 00947968

DUNS NUMBER: Redacted

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated **1st July 2024**

It's issued under the Framework Contract with the reference number RM6263 Lot 2 for the provision of Digital Specialists and Programme Deliverables.

The Parties intend that this Call-Off Contract will not oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules)).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

CALL-OFF LOT(S):

Lot 2 is the relevant Lot from Framework Schedule 1 (Specification).

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where schedules are struck through we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions) RM6263
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
 - Joint Schedules for RM6263
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 6 (Key Sub-contractors)
 - Joint Schedule 7 (Financial Difficulties)
 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Joint Schedule 12 (Supply Chain Visibility)
 - Joint Schedule 13 (Cyber Essentials)
 - Call-Off Schedules for RM6263
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 3 (Continuous Improvement)
 - Call-Off Schedule 4 (Call-Off Tender)
 - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
 - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliveries)
 - Call-Off Schedule 7 (Key Supplier Staff)
 - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
 - Call-Off Schedule 9 (Security)
 - Call-Off Schedule 10 (Exit Management)
 - Call-Off Schedule 13 (Implementation Plan and Testing) – Only identified in a Statement of Work (SOW)
 - Call-Off Schedule 14B (Service Levels and Balanced Scorecard)
 - Call-Off Schedule 15 (Call-Off Contract Management)

- Call-Off Schedule 18 (Background Checks)
 - Call-Off Schedule 20 (Call-Off Specification)
5. RM6263 Core Terms (version 3.0.11)
 6. Joint Schedule 5 (Corporate Social Responsibility) RM6263
 7. Call-Off Schedule 4 (Call-Off Tender)

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1

Changes to definitions

1. "Start Date" to be amended in Joint Schedule 1 (Definitions) as follows:

In the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form which shall be the latter of :

- (a) the date of start of a Call-Off Contract as stated in the Order Form; and
- (b) the date on which the first Statement of Work under the relevant Call-Off Contract is executed;

and in the case of a Statement of Work, the date specified in that Statement of Work.

2. "Key Staff" to be amended in Joint Schedule 1 (Definitions) as follows:

"Key Supplier Staff"

Special Term 2

A new Clause 10.2.3 shall be added to the Core Terms:

10.2.3 Each Buyer has the right to terminate a Statement of Work at any time without reason by giving the Supplier not less than 30 days' written notice.

Special Term 3

The provision of Clause 10.6.5 of the Core Terms shall be revised as follows

10.6.5 The following Clauses survive the termination or expiry of each Contract (or any individual Statement of Work): 3.2.10, 4.2, 6, 7.5, 9, 11, 12.2, 14, 15, 16, 17, 18, 31.3, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

Special Term 4

The provision of Clause 10.7.3 of the Core Terms shall be revised as follows (with changes shown in strikethrough and underline):

Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it including terminating or suspending any or all Statements of Work made under the Call-Off Contract. If the Buyer suspends a Contract and/or Statement or Work, it can provide the Deliverables itself or buy them from a third party.

Special Term 5

The following new Clauses 10.7.3A – 10.7.3D shall be added to the Core Terms:

10.7.3A Where the Buyer terminates a Statement of Work pursuant to Clause 10.7.3 under any of Clauses 10.2.2, 10.2.3, 10.4.1, 10.4.2, 10.4.3 or 20.2 or a Statement of Work expires all of the following apply:

- (a) The Buyer's payment obligations under the terminated or expired Statement of Work stop immediately.
- (b) Accumulated rights of the Parties are not affected.
- (c) The Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the termination or expiry date of the Statement of Work.
- (d) The Supplier must promptly delete or return the Government Data held or received under the relevant Statement of Work except where required to retain copies by Law.
- (e) The Supplier must promptly return any of the Buyer's property provided under the terminated or expired Statement of Work.
- (f) Except where termination of a SoW occurs under 10.2.2 or 10.2.3 the Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

10.7.3B The Supplier may also be responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables in connection with the remainder of the Statement of Work duration where the Supplier's services have been appropriately terminated in accordance with Clause 10.4.1, and the Buyer shall remain responsible for the costs of those Replacement Deliverables under any new Statement of Work or contract.

10.7.3C In addition to the consequences of termination listed in Clause 10.6.1, if either the Relevant Authority terminates a Statement of Work under Clause 10.2.3:

- (a) the Buyer must promptly pay all outstanding Charges incurred to the Supplier;
and
- (b) the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Statement of Work had not been terminated.

10.7.3D In addition to the consequences of termination listed in Clause 10.7.3A, where a Party terminates a Statement of Work under Clause 20.2 each Party must cover its own Losses.

Special Term 6- A new Clause 10 to be added to Part B: Long Form Security Requirements of Call Off schedule 9.

DWP Security and Confidentiality Requirements

- 10.1 BPSS Security level is required for all Supplier staff working under this the Call -Off Contract.
- 10.2 In the event that any security clearances other than BPSS Security level is required, this will be included in the relevant Statement of Works.
- 10.3 Call Off Schedule 9 (Security) Part B The Long Form Security Requirements will apply to the Call Off Contract.
- 10.4 In addition, the Contracting Authority requires the following clauses to be included in any resultant the Contract:

The Supplier agrees to the additional Buyer standard clauses in respect of Security Requirements listed below.

Risk Management:

- a. The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Buyer in relation to the Buyer's own risk management processes regarding the Services.
- b. For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the security requirements stipulated in this Statement of Work. Any failure by the Supplier to comply with any security requirements of this Statement of Work, shall constitute a material Default entitling the Contracting Authority to exercise its rights under clause 10.4.1 of the Core Terms.

Security Audit and Assurance:

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

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

Security Policies and Standards

- a. The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the security policies and standards set out in paragraph 4 below.
- b. Notwithstanding the foregoing, the Buyer's security requirements applicable to the SOW Deliverables may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the SOW Deliverables. Where any such change constitutes a Variation, any necessary Variation shall be agreed by the Parties in accordance with clause 24 of the Core Terms.
- c. The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

Security Policies and Standards

- a. The Buyer's security policies are published on:
DWP procurement: security policies and standards - GOV.UK (www.gov.uk)
- b. The Supplier will be required to comply with:
- Acceptable Use Policy
 - Information Security Policy
 - Physical Security Policy
 - Information Management Policy
 - Email Policy
 - Remote Working Policy
 - Social Media Policy
 - Security Classification Policy
 - HMG Personnel Security Controls – May 2018
- (published on HMG personnel security controls - GOV.UK (www.gov.uk))

Special Term 7 - A new Clause 7.6 shall be added to Core Terms:

Where the Supplier wishes to substitute any supplier staff assigned to Deliverables, the Supplier shall provide a minimum notice period of 4 weeks to the Buyer to accommodate knowledge transfer /handover unless otherwise agreed with the Buyer.

Special Term 8 - IR35 Status- The provision of Annex 2 in this Order Form shall apply in respect of any Statement of Work concluded under this Call Off Contract.

Special Term 9 – A new Clause 11 shall be added to Call Off Schedule 10 (Exit). Within 10 days of termination or expiry of the relevant Statement of Work, the Supplier shall deliver to the Buyer all equipment provided by the Buyer to the

Supplier and the Supplier Staff for use in the provision of the Services and all other materials (together with materials containing Intellectual Property Rights), access keys, documents, and information provided to the Supplier or the Supplier Staff.

The Supplier shall ensure such property shall be handed back to the Buyer in good working order (allowance shall be made for reasonable wear and tear).

Special Term 10 - Insert a new clause 1.1A below within Call-Off Schedule 14B (Service Levels and Balanced Scorecard):

“1.1A For the avoidance of doubt, pursuant to clause 1.1 of Section 2 Balanced Scorecard the parties agree that the Balanced Scorecard and key performance indicators apply to this Call Off Contract and all Statements of Work entered into by the parties. For individual Statements of Work, the parties may agree additional Service Levels under Section 1 of this Call-Off Schedule 14B.”

Special Term 11-Insert a new clause 9.8 in the Core Terms:

9.8 For individual Statements of Work, the parties may agree the application of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) to the digital Deliverables, which will be further detailed in each Statement of Work entered into between the Buyer and Supplier.

CALL-OFF START DATE:	See Special Term 1
CALL-OFF EXPIRY DATE:	30 th June 2026
CALL-OFF INITIAL PERIOD:	2 Years,0 Months
CALL-OFF OPTIONAL EXTENSION PERIOD:	0 Years, 6 Months
MINIMUM NOTICE PERIOD FOR EXTENSION(S):	3 Months
CALL-OFF CONTRACT VALUE:	£9,228,576 (ex VAT)
KEY SUB-CONTRACT PRICE:	£0

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

BUYER'S STANDARDS

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards set out in Framework Schedule 1 (Specification). The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract: Any specific buyer standards will be set out in specific SOWs

CYBER ESSENTIALS SCHEME

The Buyer requires the Supplier, in accordance with Joint Schedule 13 (Cyber Essentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£4,614,288**

CALL-OFF CHARGES

Time and Materials (T&M);

See details in Call-Off Schedule 5 (Pricing Details and Expenses Policy) for further details.

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4 and 5 (if used) in Framework Schedule 3 (Framework Prices).

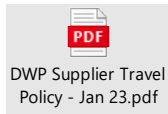
The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

REIMBURSABLE EXPENSES

DWP Expense Policy



PAYMENT METHOD

The charging method for this Call-Off Contract will be Time and Materials.

Supplier will submit completed timesheets showing consumption against contracted number of days. Timesheets will be emailed to the named individual provided in each Statement of Work weekly unless otherwise agreed in a Statement of Work.

Payment will only be made following approval of a validated timesheet.

The Supplier will issue electronic invoices monthly in arrears.

Invoices should be submitted to: APinvoices-DWP-U@gov.sscl.com.

Copy invoices will be emailed to the named individual provided for in each Statement of Work.

All invoices must meet the following requirements:

- Must include a valid purchase order number.
- All files/invoices must be in PDF format;
- One PDF per invoice – all supporting documentation must be included within the single PDF;
- Supplier should not attach additional/separate supporting documentation as a separate file.

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).

The Supplier must be able to use electronic purchase to pay (P2P) routes, including catalogue and invoicing.

The Supplier must work with DWP to set up and test all electronic P2P routes. This may involve creating technical ordering and invoicing files, including working with DWP's ERP system service supplier systems.

BUYER'S INVOICE ADDRESS:

Invoices should be submitted monthly in arrears to:

Redacted

BUYER'S AUTHORISED REPRESENTATIVE

Name: Redacted

Role: Redacted

Email: Redacted

Address: Redacted

BUYER'S ENVIRONMENTAL POLICY

The buyer is in the process of developing its environmental policy and intend to introduce this as part of the variation process.

BUYER'S SECURITY POLICY

See details in **Special Term 6** above.

SUPPLIER'S AUTHORISED REPRESENTATIVE

Redacted

SUPPLIER'S CONTRACT MANAGER

Redacted

PROGRESS REPORT FREQUENCY

Monthly or as agreed in SOW

PROGRESS MEETING FREQUENCY

Monthly or as agreed in SOW

KEY STAFF

Refer to Call off Schedule 7 "Key Supplier Staff"

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

Refer to Joint Schedule 4 "Commercial Sensitive Information"

BALANCED SCORECARD

See Call Off Schedule 14B

MATERIAL KPIs

The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14B

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)

STATEMENT OF WORKS

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	Redacted	Signature:	Redacted
Name:	Redacted	Name:	Redacted
Role:	Redacted	Role:	Redacted
Date:	Redacted	Date:	Redacted

Appendix 1

The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex 1 to the Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)).

Annex 1 (Template Statement of Work)


1. STATEMENT OF WORK ("SOW") DETAILS	
<p>Upon execution, this SOW forms part of the Call-Off Contract (reference below).</p> <p>The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.</p> <p>All SOWs must fall within the Specification and provisions of the Call-Off Contract.</p> <p>The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.</p>	
Date of SOW:	1 st July 2024
SOW Title:	Mobilisation of Resources
SOW Reference:	SOW 1
Call-Off Contract Reference:	Ecm_11664
Buyer:	Department for Work and Pensions.
Supplier:	CGI IT UK Limited
SOW Start Date:	1 st July 2024
SOW End Date:	9 th August 2024
Duration of SOW:	5 Weeks
Key Personnel (Buyer)	Redacted Redacted
Key Personnel (Supplier)	Redacted Redacted
Subcontractors	Redacted

2. CALL-OFF CONTRACT SPECIFICATION - PROGRAMME CONTEXT	
SOW Deliverables Background	The contract aims to support the DWP in maintaining business continuity for the Data Access Layer service and to continue to evolve Data Access Layer technical and service capability.
Delivery phase(s)	Mobilisation
Overview of Requirement	<p>This Statement of Work is to mobilise key resources and transition responsibilities over to them prior to incumbent Supplier departure.</p> <p>Outcome:</p> <ul style="list-style-type: none"> Buyer is assured that Supplier resources have the required skills and capabilities to enable transition and maintain business continuity so that the DAL can continue to deliver and evolve data services for DWP. <p>The Contracting Authority will provide all IT equipment to enable supplier resources to access DWP networks for the sole purpose of delivering the outcomes.</p>
Accountability Models	<p><i>Please tick the Accountability Model(s) that shall be used under this Statement of Work:</i></p> <p><i>Sole Responsibility:</i> <input type="checkbox"/></p> <p><i>Self Directed Team:</i> <input type="checkbox"/></p> <p><i>Rainbow Team:</i> X</p>

3. BUYER REQUIREMENTS – SOW DELIVERABLES	
Outcome Description	<p>Tranche A</p> <p>This tranche is made up of leadership resources to allow them to onboard to DWP and to familiarise themselves with DAL service design, ways of working, technology design, patterns and tooling, and deliverables. The intention is to provide one-to-one time with the role incumbent. The role incumbent is obliged to share background knowledge and access to appropriate documentation and strategic plans prior to operational resources being introduced at Tranche B (below).</p> <p>This Statement of Work 1 will require the future Leadership Team, working in partnership with the incumbent resources, to establish relationships across the DAL and to assume</p>

	<p>full responsibility for the role they will operate in so that transition of all roles can complete by the 9th August.</p> <p>It is assumed that the resources brought in under this statement of work will be the DAL team for future statements of work, subject to internal change within DWP.</p> <p>Redacted</p> <p>Tranche B</p> <p>This tranche onboards the remaining operational resources required to run the DAL to DWP. With the support of the Tranche A resources, they will be expected to assume full responsibility for the role they will operate in so that transition of all roles can complete by the 9th August.</p> <p>It is assumed that the resources brought in under this statement of work will be the DAL team for future statements of work, subject to internal change within DWP.</p> <p>Redacted</p>		
Milestone Ref	Milestone Description	Acceptance Criteria	Due date
MS01	Tranche A resources available to commence transition	Resources have evidence of specified level of security clearance, are suitably qualified to the specified SFIA level, at a minimum, including leadership in line with level definitions	[Start date of SoW, dependent on onboarding]
MS02	Tranche B resource available to commence transition	Resources have evidence of specified level of security clearance, are suitably qualified to specified SFIA level at a minimum	[Two weeks after state date of SoW]
MS03	Transition complete for all Tranche A and B resources	Both parties have either agreed that all transition activities have been completed, or that an appropriate recovery plan has been put in place and signed off by both parties	9 th August 2024
Delivery Plan	Digital and supplier to arrange onboarding		
Dependencies	<ul style="list-style-type: none"> Provision of DWP laptops and access to DAL development environments. Access to DWP staff and any other key stakeholders. Security clearance transfer to DWP. 		
Supplier Resource Plan	Digital and supplier to arrange onboarding		
Security Applicable to SOW:	The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security).		

	<p>If different security requirements than those set out in Call-Off Schedule 9 (Security) apply under this SOW, these shall be detailed in this SOW:</p> <p>The Supplier agrees to the additional Buyer standard clauses in respect of Security Requirements listed below.</p> <p>1. Risk Management:</p> <ol style="list-style-type: none"> The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Buyer in relation to the Buyer's own risk management processes regarding the Services. For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the security requirements stipulated in this Statement of Work. Any failure by the Supplier to comply with any security requirements of this Statement of Work, shall constitute a material Default entitling the Contracting Authority to exercise its rights under clause 10.4.1 of the Core Terms. <p>2. Security Audit and Assurance:</p> <ol style="list-style-type: none"> The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Buyer (the "Information Security Questionnaire") at least annually or at the request by the Buyer. The Supplier shall provide the completed Information Security Questionnaire to the Buyer within one calendar month from the date of request. The Buyer shall schedule regular security governance review meetings which the Supplier shall and shall procure that any Sub-contractor (as applicable) shall, attend. <p>3. Security Policies and Standards</p> <ol style="list-style-type: none"> The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the security policies and standards set out in paragraph 4 below. Notwithstanding the foregoing, the Buyer's security requirements applicable to the SOW Deliverables may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the SOW Deliverables. Where any such change constitutes a Variation, any necessary Variation shall be agreed by the Parties in accordance with clause 24 of the Core Terms. The Supplier shall and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards. <p>4. Security Policies and Standards</p> <ol style="list-style-type: none"> The Buyer's security policies are published on: DWP procurement: security policies and standards - GOV.UK (www.gov.uk) The Supplier will be required to comply with: <ul style="list-style-type: none"> Acceptable Use Policy Information Security Policy Physical Security Policy
--	---

	<ul style="list-style-type: none">• Information Management Policy• Email Policy• Remote Working Policy• Social Media Policy• Security Classification Policy• HMG Personnel Security Controls – May 2018 <p>(published on HMG personnel security controls - GOV.UK (www.gov.uk))</p>						
Cyber Security Standards	The Buyer requires the Supplier to have and maintain a Cyber Essentials Plus Certificate for the work undertaken under this SOW, in accordance with Joint Schedule 13 (Cyber Essentials Scheme).						
SOW Standards	Adhere to GDS Standards						
Performance Management	<div>See below details of Material KPIs that have a material impact on Contract performance]</div> <table><thead><tr><th>Material SLAs</th><th>Target</th><th>Measured by</th></tr></thead><tbody><tr><td>Mandatory Training – all supplier resources shall complete all DWP mandatory training within 5 working days of gaining access to DWP networks</td><td>100%</td><td>% of supplier resources providing evidence of completion of mandatory training within 5 working days</td></tr></tbody></table> <div>Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)]</div>	Material SLAs	Target	Measured by	Mandatory Training – all supplier resources shall complete all DWP mandatory training within 5 working days of gaining access to DWP networks	100%	% of supplier resources providing evidence of completion of mandatory training within 5 working days
Material SLAs	Target	Measured by					
Mandatory Training – all supplier resources shall complete all DWP mandatory training within 5 working days of gaining access to DWP networks	100%	% of supplier resources providing evidence of completion of mandatory training within 5 working days					
Additional Requirements	Annex 1 – Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.						
Key Supplier Staff	<div>Redacted</div> <div>[Indicate: whether there is any requirement to issue a Status Determination Statement]</div>						
Worker Engagement Status	<p>The provisions set out in the embedded document below shall apply to this SOW.</p> <div><p>Worker Engagement Status</p></div>						

[SOW Reporting Requirements:]	<p>Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call-Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:</p> <p>Redacted</p>
--------------------------------------	--

4. CHARGES	
Call Off Contract Charges	<p>The applicable charging method(s) for this SOW is:</p> <ul style="list-style-type: none"> • Time and Materials • Monthly in arrears based on effort in timesheets. <p>The estimated maximum value of this SOW (irrespective of the selected charging method) is The Charges detailed in the financial model shall be invoiced in accordance with Clause 4 of the Call-Off Contract.</p> <p>INVOICING: Electronic Invoices (attached to E-Mails) should be sent to:</p> <p>Redacted</p> <p>Paper invoices should be sent to;</p> <p>Redacted</p> <p>A copy should also be emailed to [TBC by Buyer]</p>
Rate Cards Applicable	<i>This SOW shall be charged in accordance with the Supplier and Subcontractor rate cards from Call-Off Schedule 5B (Pricing Details and Expenses Policy), including details of any discounts that will be applied to the work undertaken under this SOW</i>
Financial Model	N/A.
Reimbursable Expenses	<i>To be applied in accordance with the DWP Travel & Expenses policy</i>

5. SIGNATURES AND APPROVALS					
<p>Agreement of this SOW</p> <p>BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:</p>					
For and on behalf of the Supplier	<table> <tr> <td>Name and title</td><td>Redacted</td></tr> <tr> <td>Date</td><td>Redacted</td></tr> </table>	Name and title	Redacted	Date	Redacted
Name and title	Redacted				
Date	Redacted				

	Signature	Redacted
For and on behalf of the Buyer	Name and title	Redacted
	Date	Redacted
	Signature	Redacted

ANNEX 1 Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

“Processor Personnel” all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:
 - (a) “Controller” in respect of the other Party who is “Processor”;
 - (b) “Processor” in respect of the other Party who is “Controller”;
 - (c) “Joint Controller” with the other Party;
 - (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”;

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
 - (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));

- (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
 - (d) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;

- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Personal Data Breach.
8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
 - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

- (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
- 26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
- 28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- 29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

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 Relevant Authority at its absolute discretion.

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: **Redacted**
- 1.2 The contact details of the Supplier's Data Protection Officer are: **Redacted**
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">• The Supplier processes the personal information of members of the public including, but not limited to, name, nationality, immigration history, present and past addresses, criminal record, financial information, copies of passports and / or other identity documents, photographs, date of birth, reference numbers held by the DWP and / or other agencies and government departments, together with similar details for family members. Access to such data will be restricted to those Supplier Staff who need to process such information and whom must have SC level of clearance. <p>The Supplier is Controller and the Relevant Authority is Processor</p> <p><i>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data:</i></p> <ul style="list-style-type: none">• Supplier Staff details <p>The Parties are Joint Controllers</p> <p><i>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</i></p>

	<ul style="list-style-type: none"> • Business contact details of Supplier Staff for which the Supplier is the Controller • Business contact details of any directors, officers employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller <p>The Parties are Independent Controllers of Personal Data <i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> • Business contact details of Supplier Personnel for which the Supplier is the Controller, • Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller.
Duration of the Processing	The duration of this Call-Off Contract
Nature and purposes of the Processing	<p>Supplier Processing</p> <p>The Supplier is not engaged to Process Buyer Personal Data, however, the Supplier may (i) have the ability to access Buyer Personal Data by virtue of access to Buyer systems and/or (ii) receive Buyer Personal Data by virtue of correspondence between the Parties. In respect of (i), all such Buyer Personal Data will remain within the Buyer estate and the Buyer will remain responsible for all data handling controls. The Supplier will follow the Buyer's direction and guidelines on staff security clearance and processes for access to Buyer systems, including role-based access controls and security standards. Where the Supplier is required to grant user access, this will be limited to Buyer provisioned laptops and approved USB devices. Any requirement to share data externally, such as with third parties for diagnostic purposes, is not to be undertaken by the Supplier and will remain the responsibility of the Buyer. In respect of (ii), the nature of Processing by the Supplier shall be limited to the storage and retrieval of Buyer Personal Data as is necessary for the Supplier to</p>

	<p>contact and communicate with the Buyer in order to properly perform this Call-Off Contract.</p> <p>Buyer Processing</p> <p>The nature of the Processing by the Buyer shall be for the recording, storage and retrieval of Supplier Staff business Framework Schedule 6 (Order Form Template and Call-Off Schedules) Crown Copyright 2021 Framework Ref: RM6263 Project Version: v1.0 Model Version: v3.7 18 contact details and images. The purpose of such Processing by the Buyer is in order to receive the Services under this Call-Off Contract and will include such Processing as is required in accordance with Buyer standard practice in order to permit access to Buyer data, information technology systems and premises.</p>
Type of Personal Data	Name, business e-mail address, business telephone number, and in respect of Supplier Staff image.
Categories of Data Subject	Any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Staff) for which the Buyer is the controller. Supplier Staff engaged in the performance of the Supplier's duties under the Contract for which the Supplier is the Controller.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Erase or destroy appropriately as directed by the Buyer.

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Department for Work and Pensions:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

- (a) report to the other Party every 3 months on:
 - (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

- (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

- (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
 - (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
 - (j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.
- 2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.
- 3. Data Protection Breach**
- 3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:
- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

- (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
 - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
 - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's

data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. **Liabilities for Data Protection Breach**

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will

conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data

Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

ANNEX 2- IR35 STATUS

