



Ministry
of Justice

Crown Commercial Service

Call-Off Order Form Schedule 6 for RM6126 Research and Insights DPS for the provision of Research Services

con_23613

**IDAC – Pathfinder Pilots Evaluation – Strand 2
Children and Families**

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

Order Form

Applicable Framework Contract

This Order Form is for the provision of the Deliverables and dated TBC.

CONTRACT REFERENCE:	con_23613
THE BUYER:	REDACTED
BUYER ADDRESS:	Ministry of Justice, Commercial & Contract Management Directorate (CCMD), 1st floor, 5 Wellington Place, Leeds, LS1 4AP
THE CUSTOMER:	Ministry of Justice, Data and Analysis; and Court Recovery, Criminal and Family Justice Directorate
CUSTOMER ADDRESS:	102 Petty France, Westminster, London, SW1H 9AJ
THE SUPPLIER:	University of Central Lancashire
SUPPLIER ADDRESS:	Adelphi Street, Preston, PR1 2HE
REGISTRATION NUMBER:	
DUNS NUMBER:	239813694
SME STATUS	N/A
ORDER START DATE:	20 th March 2024
ORDER EXPIRY DATE:	19 th February 2025
ORDER INITIAL PERIOD:	11 months
ORDER EXTENSION PERIOD:	2 x 3 months
FINAL POSSIBLE EXPIRY DATE:	19 th August 2025
DELIVERABLES:	See details in Order Schedule 20 (Order Specification)

CALL-OFF ORDER INCORPORATED TERMS

The following documents are incorporated into this Order Contract. Where schedules are missing, those schedules are not part of the agreement and cannot be used. If the documents conflict, the following order of precedence applies:

1. This Order Form (DPS Schedule 6) including the Order Special Terms and Order Special Schedules.
2. DPS Schedule 7 (Order Procedure and Award Criteria)
3. DPS Special Terms
4. The following Schedules in equal order of precedence:
 - Joint Schedules for **RM6126 Research & Insights DPS**
 - Joint Schedule 1 (Definitions and Interpretation)
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 5 (Corporate Social Responsibility)
 - Joint-Schedule 6 (Key-Subcontractors)
 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Order Schedules for **RM6126 Research & Insights DPS**
 - Order Schedule 1 (Transparency Reports)
 - Order Schedule 2 (Staff Transfer)
 - Order Schedule 3 (Continuous Improvement)
 - Order Schedule 4 (Order Tender) Supplier Proposal
 - Order Schedule 5 (Pricing Details)
 - Order Schedule 7 (Key Supplier Staff)
 - Order Schedule 8 (Business Continuity and Disaster Recovery)
 - Order Schedule 9 (Security)
 - Order Schedule 10 (Exit Management)
 - Order Schedule 14 (Service Levels)
 - Order Schedule 20 (Order Specification)

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

CALL-OFF ORDER SPECIAL TERMS

The following Special Terms are incorporated into this Order Contract:

Costs and payment milestones

All costs must be included in the pricing submission, and any assumptions made in relation to these costs must be clearly indicated.

These rates **MUST** be fixed for the term of the contract.

REDACTED

Payment Milestones

Milestone and percentage of payment	Milestone	Expected date 2024
REDACTED	Research sign off	May
REDACTED	On completion of 50% of fieldwork	July
REDACTED	On completion of fieldwork	October
REDACTED	On delivery of the initial draft report	September
REDACTED	On acceptance of final outputs	December

Suggested Project Timeline

Stage	Suggested month of completion 2024/25
Project initiation meeting	March 2024
Finalise research approach	March 2024
Submission for ethical approval	March 2024
Agree research tools, topics guides and consent forms	March to April 2024
Stakeholder meetings	March 2024
Participant recruitment	May 2024
Fieldwork	May to October 2024
Agreements and/or approvals agreed and signed off	End of June 2024

Analysis	May to November 2024
Interim findings presentation	w/c 15 th or 22 nd July 2024
Co-production workshops	September to October 2024
Final report presentations: MoJ	w/c 28 th October 2024
First draft of final report	11 th November 2024
Final report presentation: Key stakeholders	w/c 25 th November 2024
Final report and technical annex	20 th December 2024
Child focused output and policy briefing	w/c 6 th January 2025

The Intellectual Property Rights of all products and reporting from the contract will belong to MoJ.

Ownership of data and Intellectual Property from this project will be retained by the Authority and the Supplier will be required to provide assurance to the Authority that all data will be destroyed within a reasonable timeframe from completion of the project


Order Schedule 14 (Service Levels)

Project management	<p>Supplier Obligations</p> <ul style="list-style-type: none"> • The Supplier should nominate a project manager who is the primary contact for the Authority. • The project manager should have sufficient experience, seniority and time allocated to manage the project effectively. They will be responsible for managing the project and ensuring Authority is kept up to date on project progress. • It is expected that, following a project inception meeting, regular weekly contact will take place between the Supplier and the Authority by telephone, email and/or virtual meetings. <p>The Supplier must:</p>
---------------------------	---

	<ul style="list-style-type: none"> • Identify the project team that will be involved in working on the project, outlining their grade or experience, number of days to be spent on the project, skills, expertise, and nature of their involvement in the research. • Outline how the contract will be delivered in the event of staff changes during the project. • Provide details of how they will keep the MoJ updated on the progress and emerging findings of the project. • Describe in detail how they will manage this project to ensure that it runs smoothly. • Identify risks associated with the successful completion of the research and how they plan to mitigate them. • Provide details about any sub-contractors or external experts they will be using and for which parts of the project. <p>Quality Assurance</p> <ul style="list-style-type: none"> • The Supplier must provide details of the quality assurance procedures they have in place for the duration of the contract. <p>Risk Management</p> <p>Suppliers must:</p> <ul style="list-style-type: none"> • Identify and assess the risks associated with undertaking the research. • Outline proposals for managing and overcoming risks. • Provide a full risk register for all elements of the project. • Outline a process to ensure the Authority is updated as issues emerge, and escalation is required. <p>Reporting</p> <p>Supplier will be expected to:</p> <ul style="list-style-type: none"> • Proactively engage with the Authority's designated project manager throughout the contract. • Take reasonable steps to monitor progress and timings for the duration of the project. • Provide fortnightly progress updates to the Authority. • Keep the Authority updated as issues emerge and need to be escalated.
Performance Monitoring	<p>The Supplier will be expected to engage with the Authority in line with the dates agreed between the Authority and the Supplier agreed at the project inception meeting.</p> <p>There will be</p>

	<ul style="list-style-type: none"> • Fortnightly progress meetings with the Supplier's nominated project manager, with progress updates. • Monthly meetings between the Authority and Supplier. <p>This is subject to change as the project progresses or should this be requested by the Authority or Supplier.</p>
--	--

REPORTING	
PROGRESS REPORT FREQUENCY	Fortnightly
PROGRESS MEETING FREQUENCY	Monthly

PAYMENT METHOD
<p>All invoices must be sent, quoting a valid purchase order number (PO Number) Within 10 Working Days* of receipt of your countersigned copy of this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.</p> <p>Ministry of Justice (including its various departments, agencies and arm's-length bodies) now uses the Basware Network to trade electronically with our suppliers.</p> <p>If you are not currently a supplier to the Ministry of Justice or your details are out of date, we will need to do a supplier set up.</p> <p>To ensure that both the Ministry of Justice and our suppliers can maximise the benefits from using Basware, we will require you to register with Basware. Please see the attached Basware letter for further information.</p> <div style="text-align: center;">  </div> <p>Welcome-to-Basware -eMarketplace-supplier</p>

There are 3 ways suppliers can submit invoices can be submitted to MoJ for payment:

1. Paper/PDF	invoices are posted/emailed to the shared service centre. On receipt, the invoice is scanned and loaded onto SOP using Optical Character Recognition (OCR) software.
2. Electronic invoice file (Tech 11)	invoices are emailed to the shared service centre in a specific text file format that SOP can read without the need of OCR software. Engagement is required with the supplier before invoices are accepted in this format.
3. Basware	invoices are submitted via the Basware supplier portal and are then transmitted electronically into SOP via XML. Suppliers must be onboarded to Basware before they submit invoices in this method.

What you need to do

Except for those submitted via Basware, all invoice should be sent directly to SSCL (see below)

Suppliers providing electronic invoice files will be given a specific email for their invoices once onboarded.

Invoice minimum requirements

To enable successful processing, all invoices submitted to MoJ must clearly state the word 'invoice' and contain the following:

- a unique identification number (invoice number)
- your company name, address and contact information
- the name and address of the department/agency you're invoicing
- a clear description of what you're charging for
- the date the goods or service were provided (supply date)
- the date of the invoice
- the amount(s) being charged
- VAT amount if applicable
- the total amount owed
- a cost centre code (available from your MoJ business contact) or a valid purchase order (PO) number

If any of the above information is missing from your invoice, it will be returned to you.

Invoices relating to a purchase order

In addition to the minimum requirements above, invoices relating to a PO must not contain any lines for items which are not on the purchase order. If this occurs, your invoice will be returned to you.

Speak to the business contact on the purchase order if there are any additional items/services which you need to invoice for.

Invoice submission by email

All invoices submitted by email must meet the following criteria:

- Email size must not exceed 4mb
- 1 invoice per file attachment (PDF), multiple invoices can be attached as separate files
- Any supporting information, backing data etc. must be contained within the invoice PDF file

Failure to meet these criteria may result in not all your invoices being processed, or your invoice(s) being returned to you.

CUSTOMER'S INVOICE ADDRESS:

The email and postal address for PDF and paper invoices can be found here.

<https://www.gov.uk/government/organisations/ministry-of-justice/about/procurement>

AUTHORITY'S ENVIRONMENTAL POLICY

Embedding sustainability on the MOJ estate, Published 26 March 2018, Last updated 4 October 2021, available online at: <https://www.gov.uk/guidance/ministry-of-justice-and-the-environment>

AUTHORITY'S SECURITY POLICY

Cyber and Technical Security Guidance, 14 December 202, available online at: [Security Guidance \(justice.gov.uk\)](https://www.justice.gov.uk/security-guidance).

AUTHORITY'S AUTHORISED REPRESENTATIVE

Name:	REDACTED
Role:	REDACTED
Email:	REDACTED
Address:	REDACTED

AUTHORITIES KEY STAFF

Key Role	Key Staff (Name & email)	Contact Details
REDACTED	REDACTED	REDACTED


AUTHORITIES CONTRACT MANAGER	
Name	REDACTED
Role:	REDACTED
Email:	REDACTED
Address:	REDACTED

SUPPLIER'S AUTHORISED REPRESENTATIVE	
Name:	REDACTED
Role:	REDACTED
Email:	REDACTED
Address:	REDACTED

SUPPLIER'S KEY STAFF – See DPS Order Schedule 7 - Key Supplier Staff					
Key Role		Key Staff		Contact Details	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	

SUPPLIER'S CONTRACT MANAGER	
Name:	REDACTED
Role:	REDACTED
Email:	REDACTED
Address:	REDACTED

KEY SUBCONTRACTOR(S) – See DPS Joint Schedule 6 - Key Subcontractors-v1.0 (IF APPLICABLE)		
Key Role	Key Staff (Name & email)	Contact Details
REDACTED	REDACTED	REDACTED

INFORMATION	
MAXIMUM LIABILITY The limitation of liability for this Order Contract is as below and not as is stated in Clause 11.2 of the Core Terms.	Each Party's total aggregate liability in each Contract Year under each Order Contract (whether in tort, contract or otherwise) is no more than one hundred and fifty percent (150%) of the Estimated Yearly Charges unless specified in the Order Form.
CALL-OFF ORDER CHARGES	See details in Order Schedule 5 (Pricing Details)
REIMBURSABLE EXPENSES	Not permitted unless approved in advance by the Customer and in line with MoJ Policy.  Travel and subsistence policy and
DPS FILTER CATEGORY(IES):	Not applicable
E-AUCTIONS	Not applicable
SERVICE CREDITS	Not applicable
ADDITIONAL INSURANCES	Not applicable
GUARANTEE	Not applicable
COMMERCIALLY SENSITIVE INFORMATION	See DPS Joint Schedule 4 - Commercially Sensitive Information v1.0 <i>For example:</i> Daily rates Client organisation names Client contact information Experience descriptions Staff information (including all information contained within, but not limited to biographies and CV's)

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in DPS Order Schedule 4 - Order Tender v1.0 REDACTED CONFIDENTIAL INFORMATION

Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

For and on behalf of the Buyer: Ministry of Justice	
Signature:	REDACTED
Name:	REDACTED
Role:	REDACTED
Date:	REDACTED

For and on behalf of the Supplier: University of Central Lancashire	
Signature:	REDACTED
Name:	REDACTED
Role:	REDACTED
Date:	REDACTED

Contents

JOINT SCHEDULES FOR RM6126 RESEARCH & INSIGHTS DPS	
<u>DPS Schedule 7 (Order Procedure and Award Criteria)</u>	
<u>DPS Joint Schedule 1 - Definitions v1.0</u>	
<u>DPS Joint Schedule 2 (Variation Form)</u>	
<u>DPS Joint Schedule 3 (Insurance Requirements)</u>	
<u>DPS Joint Schedule 4 (Commercially Sensitive Information)</u>	CONFIDENTIAL
<u>DPS Joint Schedule 5 (Corporate Social Responsibility)</u>	
<u>DPS Joint-Schedule 6 (Key-Subcontractors)</u>	CONFIDENTIAL
<u>DPS Joint Schedule 10 (Rectification Plan)</u>	
<u>DPS Joint Schedule 11 (Processing Data)</u>	

ORDER SCHEDULES FOR RM6126 RESEARCH & INSIGHTS DPS	
<u>DPS Order Schedule 2 (Staff Transfer)</u>	
<u>DPS Order Schedule 3 (Continuous Improvement)</u>	
<u>DPS Order Schedule 4 (Order Tender) - (Supplier Proposal)</u>	CONFIDENTIAL
<u>DPS Order Schedule 5 (Pricing Details)</u>	CONFIDENTIAL
<u>DPS Order Schedule 7 (Key Supplier Staff)</u>	CONFIDENTIAL
<u>DPS Order Schedule 8 (Business Continuity and Disaster Recovery)</u>	
<u>DPS Order Schedule 9 (Security)</u>	
<u>DPS Order Schedule 10 - Exit Management v1.1</u>	
<u>DPS Order Schedule 14 - Service Levels v1.1</u>	
<u>DPS Order Schedule 20 - Specification v1.0</u>	

Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In each Contract, unless the context otherwise requires:
 - 1.3.1 the singular includes the plural and vice versa; 1.3.2 reference to a gender includes the other gender and the neuter; 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;
 - 1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
 - 1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";
 - 1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
 - 1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;
 - 1.3.8 references to "**Clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
 - 1.3.9 references to "**Paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;
 - 1.3.10 references to a series of Clauses or Paragraphs shall be inclusive

of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract; and 1.3.12 where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and " Achieved ", " Achieving " and " Achievement " shall be construed accordingly;
"Additional Insurances"	insurance requirements relating to an Order Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
"Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-amsupplier/management-information/admin-fees ;
"Affected Party"	the party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Annex"	extra information which supports a Schedule;
"Approval"	the prior written consent of the Buyer and " Approve " and " Approved " shall be construed accordingly;
"Audit"	<p>the Relevant Authority's right to:</p> <ul style="list-style-type: none">a) verify the accuracy of the Charges and any other amounts payable by a Buyer under an Order Contract (including proposed or actual variations to them in accordance with the Contract);b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services;c) verify the Open Book Data;d) verify the Supplier's and each Subcontractor's compliance with the applicable Law;e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;

	<ul style="list-style-type: none"> f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; k) verify the accuracy and completeness of any Management Information delivered or required by the DPS Contract;
"Auditor"	<ul style="list-style-type: none"> a) the Buyer's internal and external auditors; b) the Buyer's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Buyer to carry out audit or similar review functions; and f) successors or assigns of any of the above;
"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;

"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Order Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the DPS Contract initially identified in the DPS Appointment Form and subsequently on the Platform;
"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: <ul style="list-style-type: none"> a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Order Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Order Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
"Commercially Sensitive Information"	the Confidential Information listed in the DPS Appointment Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority,

	would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as " confidential ") or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
"Contract"	either the DPS Contract or the Order Contract, as the context requires;
"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"Contract Period"	the term of either a DPS Contract or Order Contract from the earlier of the: <ul style="list-style-type: none"> a) applicable Start Date; or b) the Effective Date until the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and " Controlled " shall be construed accordingly;
"Controller"	has the meaning given to it in the GDPR;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under DPS Contracts and Order Contracts;
"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: <ul style="list-style-type: none"> a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man Day, of engaging the Supplier Staff, including:

	<p>i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances;</p> <p>v) any other contractual employment benefits;</p> <p>vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and</p> <p>ix) reasonable recruitment costs, as agreed with the Buyer;</p> <p>b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</p> <p>c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables;</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but</p> <p>excluding:</p> <p>a) Overhead;</p> <p>b) financing or similar costs;</p> <p>c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Order Contract Period whether in relation to Supplier Assets or otherwise;</p> <p>d) taxation;</p> <p>e) fines and penalties;</p> <p>f) amounts payable under Order Schedule 16 (Benchmarking) where such Schedule is used; and</p> <p>g) non-cash items (including depreciation, amortisation, impairments and movements in provisions);</p>
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments
	and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;

"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under an Order Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Levy"	has the meaning given to it in Paragraph 8.1.1 of DPS Schedule 5 (Management Levy and Information);
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Mobilisation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of an Order Contract as confirmed and accepted by the Buyer by either (a) confirmation in writing to the Supplier; or (b) where Order Schedule 13 (Implementation Plan and Testing) is used, issue by the Buyer of a Satisfaction Certificate. " Deliver " and " Delivered " shall be construed accordingly;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof
	will be unavailable (or could reasonably be anticipated to be unavailable) for the period specified in the Order Form (for the purposes of this definition the " Disaster Period ");

"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
"Dispute"	any claim, dispute or difference arises out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	<p>descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:</p> <p>a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables;</p> <p>b) is required by the Supplier in order to provide the Deliverables; and/or has been or shall be generated for the purpose of providing the Deliverables;</p>
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"DPA 2018"	a) the Data Protection Act 2018;
"DPS"	the dynamic purchasing system operated by CCS in accordance with Regulation 34 that this DPS Contract governs access to;
"DPS Application"	the application submitted by the Supplier to CCS and annexed to or referred to in DPS Schedule 2 (DPS Application);
"DPS Appointment Form"	the document outlining the DPS Incorporated Terms and crucial information required for the DPS Contract, to be executed by the Supplier and CCS and subsequently held on the Platform;
"DPS Contract"	the dynamic purchasing system access agreement established between CCS and the Supplier in accordance with Regulation 34 by the DPS Appointment Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;

"DPS Contract Period"	the period from the DPS Start Date until the End Date or earlier termination of the DPS Contract;
"DPS Expiry Date"	the date of the end of the DPS Contract as stated in the DPS Appointment Form;
"DPS Incorporated Terms"	the contractual terms applicable to the DPS Contract specified in the DPS Appointment Form;
"DPS Initial Period"	the initial term of the DPS Contract as specified in the DPS Appointment Form;
"DPS Optional Extension Period"	such period or periods beyond which the DPS Initial Period may be extended up to a maximum of the number of years in total specified in the DPS Appointment Form;
"DPS Pricing"	the maximum price(s) applicable to the provision of the Deliverables set out in DPS Schedule 3 (DPS Pricing);
"DPS Registration"	the registration process a Supplier undertakes when submitting its details onto the Platform;
"DPS SQ Submission"	the Supplier's selection questionnaire response;
"DPS Special Terms"	any additional terms and conditions specified in the DPS Appointment Form incorporated into the DPS Contract;
"DPS Start Date"	the date of start of the DPS Contract as stated in the DPS Appointment Form;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;
"EIR"	the Environmental Information Regulations 2004;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
"End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and
	minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;

"Estimated Year 1 Contract Charges"	the anticipated total charges payable by the Supplier in the first Contract Year specified in the Order Form; a)
"Estimated Yearly Charges"	<p>means for the purposes of calculating each Party's annual liability under clause 11.2 :</p> <p>i) in the first Contract Year, the Estimated Year 1 Contract Charges; or</p> <p>ii) in any subsequent Contract Years, the Charges paid or payable in the previous Contract Year; or</p> <p>iii) after the end of the Contract, the Charges paid or payable in the last Contract Year during the Contract Period;</p>
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
"Expiry Date"	the DPS Expiry Date or the Order Expiry Date (as the context dictates);
"Extension Period"	the DPS Optional Extension Period or the Order Optional Extension Period as the context dictates;
"Filter Categories"	the number of categories specified in DPS Schedule 1 (Specification), if applicable;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	<p>any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from:</p> <p>a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract;</p> <p>b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare;</p>

	<p>c) acts of a Crown Body, local government or regulatory bodies;</p> <p>d) fire, flood or any disaster; or</p> <p>e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding:</p> <p>i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned;</p> <p>and</p> <p>any failure of delay caused by a lack of funds;</p>
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"GDPR"	i) the General Data Protection Regulation (Regulation (EU) 2016/679);
"General Anti-Abuse Rule"	<p>b) the legislation in Part 5 of the Finance Act 2013; and</p> <p>any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions;</p>
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	a) goods made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the 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 within the relevant industry or business sector;
"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	<p>the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:</p> <p>i) are supplied to the Supplier by or on behalf of the Authority; or</p>
	the Supplier is required to generate, process, store or transmit pursuant to a Contract;

"Government Procurement Card"	the Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/governmentprocurement-card--2 ;
"Guarantor"	i) the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the DPS Pricing/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and <p>such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;</p>
"Implementation Plan"	the plan for provision of the Deliverables set out in Order Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Indemnifier"	a) a Party from whom an indemnity is sought under this Contract;
"Independent Control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "Independent Controller" shall be construed accordingly;
"Indexation"	the adjustment of an amount or sum in accordance with DPS Schedule 3 (DPS Pricing) and the relevant Order Form;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;

"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of a Contract specified on the Platform or the Order Form, as the context requires;
"Insolvency Event"	<p>a) in respect of a person:</p> <p>b) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or c) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or</p> <p>d) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or</p> <p>e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or</p> <p>f) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or</p> <p>g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or</p> <p>h) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or</p> <p>i) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or</p> <p>any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;</p>
"Installation Works"	all works which the Supplier is to carry out at the beginning of the Order Contract Period to install the Goods in accordance with the Order Contract;
"Intellectual Property Rights" or "IPR"	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 or

	<p>business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;</p> <p>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; and</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
"Invoicing Address"	the address to which the Supplier shall Invoice the Buyer as specified in the Order Form;
"IPR Claim"	a) any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	<p>the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at:</p> <p>https://www.gov.uk/guidance/ir35-find-out-if-it-applies;</p>
"Joint Controller Agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (<i>Processing Data</i>);
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
"Key Personnel"	the individuals (if any) identified as such in the Order Form;
"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	<p>any Subcontractor:</p> <p>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or</p> <p>c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Order Contract, and the Supplier shall list all such Key Subcontractors on the Platform and in the Key Subcontractor Section in the Order Form;</p>
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;

"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "Loss" shall be interpreted accordingly;
"Man Day"	7.5 Man Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
"Man Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;
"Management Information"	the management information specified in DPS Schedule 5 (Management Levy and Information);
"Management Levy"	the sum specified on the Platform payable by the Supplier to CCS in accordance with DPS Schedule 5 (Management Levy and Information);
"Marketing Contact"	shall be the person identified in the DPS Appointment Form;
"MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period;
"MI Failure"	means when an MI report: <ul style="list-style-type: none"> a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or is not submitted by the reporting date (including where a declaration of no business should have been filed);
"MI Report"	means a report containing Management Information submitted to the Authority in accordance with DPS Schedule 5 (Management Levy and Information);
"MI Reporting Template"	a) means the form of report set out in the Annex to DPS Schedule 5 (Management Levy and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task described in the Mobilisation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Mobilisation Plan by which the Milestone must be Achieved;
"Month"	a calendar month and "Monthly" shall be interpreted accordingly;

"National Insurance"	contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	<p>a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or</p> <p>b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;</p>
"Occasion of Tax Non – Compliance"	<p>where:</p> <p>a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:</p> <p>i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or</p> <p>any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;</p>
"Open Book Data"	<p>complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Order Contract, including details and all assumptions relating to:</p> <p>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;</p> <p>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:</p> <p>i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;</p> <p>ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency)</p>

	<p>together with a list of agreed rates against each manpower grade;</p> <p>iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and</p> <p>iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads;</p> <p>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</p> <p>e) the Supplier Profit achieved over the DPS Contract Period and on an annual basis;</p> <p>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;</p> <p>g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and</p> <p>the actual Costs profile for each Service Period;</p>
"Order"	a) means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Contract"	b) the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the DPS Contract), which consists of the terms set out and referred to in the Order Form;
"Order Contract Period"	the Contract Period in respect of the Order Contract;
"Order Expiry Date"	the date of the end of an Order Contract as stated in the Order Form;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create an Order Contract;
"Order Form Template"	the template in DPS Schedule 6 (Order Form Template and Order Schedules);
"Order Incorporated Terms"	the contractual terms applicable to the Order Contract specified under the relevant heading in the Order Form;
"Order Initial Period"	the Initial Period of an Order Contract specified in the Order Form;
"Order Optional Extension Period"	such period or periods beyond which the Order Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form;
"Order Procedure"	the process for awarding an Order Contract pursuant to Clause 2 (How the contract works) and DPS Schedule 7 (Order Procedure);

"Order Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Order Contract;
"Order Start Date"	the date of start of an Order Contract as stated in the Order Form;
"Order Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following an Order Procedure and set out at Order Schedule 4 (Order Tender);
"Other Contracting Authority"	any actual or potential Buyer under the DPS Contract;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the DPS Contract, CCS or the Supplier, and in the in the context of an Order Contract the Buyer or the Supplier. "Parties" shall mean both of them where the context permits;
"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the DPS Contract set out in DPS Schedule 4 (DPS Management);
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
"Platform"	the online application operated on behalf of CCS to facilitate the technical operation of the DPS;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies ;
"Processing"	has the meaning given to it in the GDPR;
"Processor"	has the meaning given to it in the GDPR;

"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;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
"Prohibited Acts"	<p>a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:</p> <ul style="list-style-type: none"> i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; <p>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or</p> <p>c) committing any offence:</p> <ul style="list-style-type: none"> i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
"Protective Measures"	appropriate technical and organisational measures which may include pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in DPS Schedule 9 (Cyber Essentials), if applicable, in the case of the DPS Contract or Order Schedule 9 (Security), if applicable, in the case of an Order Contract;

"Recall"	a) a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	<p>the Supplier's plan (or revised plan) to rectify its breach using the template in Joint Schedule 10 (Rectification Plan Template) which shall include:</p> <p>a) full details of the Default that has occurred, including a root cause analysis;</p> <p>b) the actual or anticipated effect of the Default; and</p> <p>the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);</p>
"Rectification Plan Process"	the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process);
"Regulations"	a) the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
"Reimbursable Expenses"	<p>the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:</p> <p>a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and subsistence expenses incurred by Supplier Staff whilst performing</p> <p>the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;</p>
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	<p>a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);</p> <p>b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and</p>
	c) information derived from any of the above;

"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Order Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in Part B of Order Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Order Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
"Schedules"	any attachment to a DPS or Order Contract which contains important information specific to each aspect of buying and selling;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Order Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	means the certificate in the form as set out in DPS Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;

"Service Levels"	any service levels applicable to the provision of the Deliverables under the Order Contract (which, where Order Schedule 14 (Service Credits) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Order Form;
"Services"	services made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Special Terms"	a) any additional Clauses set out in the DPS Appointment Form or Order Form which shall form part of the respective Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in DPS Schedule 1 (Specification), as may, in relation to an Order Contract, be supplemented by the Order Form;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in DPS Schedule 1 (Specification);

	<p>c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;</p> <p>relevant Government codes of practice and guidance applicable from time to time;</p>
"Start Date"	in the case of the DPS Contract, the date specified on the DPS Appointment Form, and in the case of an Order Contract, the date specified in the Order Form;
"Statement of Requirements"	a) a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Order Procedure;
"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	<p>any contract or agreement (or proposed contract or agreement), other than an Order Contract or the DPS Contract, pursuant to which a third party:</p> <p>a) provides the Deliverables (or any part of them);</p> <p>b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);</p>
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	a) any third party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the DPS Appointment Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Order Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the DPS Appointment Form, or later defined in an Order Contract;
"Supplier's Confidential Information"	<p>a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier;</p> <p>b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract;</p> <p>Information derived from any of (a) and (b) above;</p>

"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Order Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	a) the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Order Contract;
"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of an Order Contract for the relevant period;
"Supplier Profit Margin"	a) in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supply Chain Information Report Template"	the document at Annex 1 of Joint Schedule 12 (Supply Chain Visibility);
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Order Contract detailed in the information are properly payable;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
"Test Issue"	any variance or non-conformity of the Deliverables or Deliverables from their requirements as set out in an Order Contract;
"Test Plan"	a plan: a) for the Testing of the Deliverables; and setting out other agreed criteria related to the achievement of Milestones;

"Tests and Testing"	any tests required to be carried out pursuant to an Order Contract as set out in the Test Plan or elsewhere in an Order Contract and "Tested" shall be construed accordingly;
"Third Party IPR"	a) Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Order Schedule 1 (Transparency Reports);
"Variation"	has the meaning given to it in Clause 24 (Changing the contract);
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and
"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	[delete] as applicable: CCS / Buyer] ("CCS" "the Buyer") And [insert] name of Supplier] ("the Supplier")	
Contract name:	[insert] name of contract to be changed] ("the Contract")	
Contract reference number:	[insert] contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete] as applicable: CCS/Buyer/Supplier]	
Variation number:	[insert] variation number]	
Date variation is raised:	[insert] date]	
Proposed variation		
Reason for the variation:	[insert] reason]	
An Impact Assessment shall be provided within:	[insert] number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert] assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> [CCS/Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause] 	
Financial variation:	Original Contract Value:	£ [insert] amount]
	Additional cost due to variation:	£ [insert] amount]
	New Contract value:	£ [insert] amount]

1. 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 **[delete]** as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. 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 **[delete]** as applicable: CCS / 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

Joint Schedule 3 (Insurance Requirements)

The insurance you need to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under an Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the DPS Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Order Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

What happens if you aren't insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

Evidence of insurance you must provide

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or nonrenewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant

Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the DPS Start Date in accordance with this Schedule:
 - 1.1 professional indemnity insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] one million pounds (£1,000,000);
 - 1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than one million pounds (£1,000,000); and
 - 1.3 employers' liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000).

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.

(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at

<https://www.modernslaveryhelpline.org/report> or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

- 3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world.
- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world.
- 3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
- 3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;
- 3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

- 4.1.1 ensure that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;
- 4.1.3 ensure that all workers are provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;
- 4.1.4 not make deductions from wages:
 - (a) as a disciplinary measure
 - (b) except where permitted by law; or
 - (c) without expressed permission of the worker concerned;

- 4.1.5 record all disciplinary measures taken against Supplier Staff; and
- 4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

- 5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
- 5.1.2 ensure that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- 5.1.3 ensure that use of overtime is used responsibly, taking into account:
 - (a) the extent;
 - (b) frequency; and
 - (c) hours worked;

by individuals and by the Supplier Staff as a whole;

- 5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
- 5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
 - 5.3.1 this is allowed by national law;
 - 5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
 - 5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and
 - 5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.
- 5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

6. Sustainability

- 6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[Guidance: Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[add date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[add cause]		
Anticipated impact assessment:	[add impact]		
Actual effect of Default:	[add effect]		
Steps to be taken to rectification:	Steps	Timescale	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[...]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	Steps	Timescale	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[...]	[date]	

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[add reasons]		
Signed by [CCS/Buyer]		Date:	

Order Schedule 3 (Continuous Improvement)

1 BUYER'S RIGHTS

- 1.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2 SUPPLIER'S OBLIGATIONS

- 2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.
- 2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.
- 2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year ("**Continuous Improvement Plan**") for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:
 - 2.3.1 identifying the emergence of relevant new and evolving technologies;
 - 2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);
 - 2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and
 - 2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.
- 2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.
- 2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

- 2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.
- 2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.
- 2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
 - 2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and
 - 2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.
- 2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.
- 2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.
- 2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.
- 2.12 At any time during the Contract Period of the Order Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Order Schedule 8 (Business Continuity and Disaster Recovery)

3 Definitions

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

"BCDR Plan"	has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 4.3.2 of this Schedule;
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 4.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 8.2 of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 8.3 of this Schedule;

4 BCDR Plan

- 4.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
- 4.2 At least ninety (90) Working Days after the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a "BCDR Plan"), which shall detail the processes and arrangements that the Supplier shall follow to:
 - 4.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

- 4.2.2 the recovery of the Deliverables in the event of a Disaster
- 4.3 The BCDR Plan shall be divided into three sections:
- 4.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;
 - 4.3.2 Section 2 which shall relate to business continuity (the "**Business Continuity Plan**"); and
 - 4.3.3 Section 3 which shall relate to disaster recovery (the "**Disaster Recovery Plan**").
- 4.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

5 General Principles of the BCDR Plan (Section 1)

- 5.1 Section 1 of the BCDR Plan shall:
- 5.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
 - 5.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
 - 5.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
 - 5.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
 - 5.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;
 - 5.1.6 contain a risk analysis, including:
 - (a) failure or disruption scenarios and assessments of likely frequency of occurrence;
 - (b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
 - (c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
 - (d) a business impact analysis of different anticipated failures or disruptions;
 - 5.1.7 provide for documentation of processes, including business processes, and procedures;

- 5.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
- 5.1.9 identify the procedures for reverting to "normal service";
- 5.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;
- 5.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and
- 5.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.
- 5.2 The BCDR Plan shall be designed so as to ensure that:
 - 5.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;
 - 5.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;
 - 5.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and
 - 5.2.4 it details a process for the management of disaster recovery testing.
- 5.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.
- 5.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service Levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

6 Business Continuity (Section 2)

- 6.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:
 - 6.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
 - 6.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.
- 6.2 The Business Continuity Plan shall:
 - 6.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;
 - 6.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

- 6.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
- 6.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

7 Disaster Recovery (Section 3)

- 7.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 7.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
 - 7.2.1 loss of access to the Buyer Premises;
 - 7.2.2 loss of utilities to the Buyer Premises;
 - 7.2.3 loss of the Supplier's helpdesk or CAFM system;
 - 7.2.4 loss of a Subcontractor;
 - 7.2.5 emergency notification and escalation process;
 - 7.2.6 contact lists;
 - 7.2.7 staff training and awareness;
 - 7.2.8 BCDR Plan testing;
 - 7.2.9 post implementation review process;
 - 7.2.10 any applicable Performance Indicators with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
 - 7.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
 - 7.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
 - 7.2.13 testing and management arrangements.

8 Review and changing the BCDR Plan

- 8.1 The Supplier shall review the BCDR Plan:
 - 8.1.1 on a regular basis and as a minimum once every six (6) Months;
 - 8.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph **Error! Reference source not found.**; and

- 8.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 8.1.1 and 8.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.
- 8.2 Each review of the BCDR Plan pursuant to Paragraph 8.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.
- 8.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.
- 8.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 8.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

9 Testing the BCDR Plan

- 9.1 The Supplier shall test the BCDR Plan:
- 9.1.1 regularly and in any event not less than once in every Contract Year;
- 9.1.2 in the event of any major reconfiguration of the Deliverables
- 9.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).
- 9.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer

unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

- 9.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
- 9.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
- 9.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:
 - 9.5.1 the outcome of the test;
 - 9.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
 - 9.5.3 the Supplier's proposals for remedying any such failures.
- 9.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

10 Invoking the BCDR Plan

- 10.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

11 Circumstances beyond your control

- 11.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Order Schedule 9 (Security)

[Guidance Note: Buyer to select whether or when Part A (Short Form Security Requirements) or Part B (Long Form Security Requirements) should apply. Part B should be considered where there is a high level of risk to personal or sensitive data.]

Part A: Short Form Security Requirements

12 Definitions

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

"Breach of Security"

the occurrence of:

- a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or
- b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,

in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;

"Security Management Plan"

the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time;

13 Complying with security requirements and updates to them

13.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

13.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security

Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

- 13.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 13.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.
- 13.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

14 Security Standards

- 14.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
- 14.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
 - 14.2.1 is in accordance with the Law and this Contract;
 - 14.2.2 as a minimum demonstrates Good Industry Practice;
 - 14.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
 - 14.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
- 14.3 The references to standards, guidance and policies contained or set out in Paragraph 14.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
- 14.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

15 Security Management Plan

15.1 Introduction

- 15.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

15.2 Content of the Security Management Plan

15.2.1 The Security Management Plan shall:

- (a) comply with the principles of security set out in Paragraph **Error! Reference source not found.** and any other provisions of this Contract relevant to security;
- (b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
- (c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- (d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- (e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
- (f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
- (g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

15.3 Development of the Security Management Plan

15.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 15.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

15.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 15.3.1, or any subsequent revision to it in accordance with Paragraph 15.4, is Approved it will be adopted

immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

15.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 15.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 15.2 shall be deemed to be reasonable.

15.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 15.3.2 or of any change to the Security Management Plan in accordance with Paragraph 15.4 shall not relieve the Supplier of its obligations under this Schedule.

15.4 Amendment of the Security Management Plan

15.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

- (a) emerging changes in Good Industry Practice;
- (b) any change or proposed change to the Deliverables and/or associated processes;
- (c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;
- (d) any new perceived or changed security threats; and
- (e) any reasonable change in requirements requested by the Buyer.

15.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

- (a) suggested improvements to the effectiveness of the Security Management Plan;
- (b) updates to the risk assessments; and
- (c) suggested improvements in measuring the effectiveness of controls.

15.4.3 Subject to Paragraph 15.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 15.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

15.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

16 Security breach

16.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

16.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 16.1, the Supplier shall:

16.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- (a) minimise the extent of actual or potential harm caused by any Breach of Security;
- (b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
- (c) prevent an equivalent breach in the future exploiting the same cause failure; and
- (d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

16.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Part B: Long Form Security Requirements

17 Definitions

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

"Breach of Security"

means the occurrence of:

- a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or
- b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,

in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;

"ISMS"

the information security management system and process developed by the Supplier in accordance with Paragraph 19 (ISMS) as updated from time to time in accordance with this Schedule; and

"Security Tests"

tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

18 Security Requirements

18.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

18.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

18.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

18.3.1 [insert security representative of the Buyer]

18.3.2 [insert security representative of the Supplier]

- 18.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.
- 18.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
- 18.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.
- 18.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.
- 18.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

19 Information Security Management System (ISMS)

- 19.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs **Error! Reference source not found.** to 19.6.
- 19.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.
- 19.3 The Buyer acknowledges that;
 - 19.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and
 - 19.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.
- 19.4 The ISMS shall:
 - 19.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;
 - 19.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph **Error! Reference source not found.**;

19.4.3 at all times provide a level of security which:

- (a) is in accordance with the Law and this Contract;
- (b) complies with the Baseline Security Requirements;
- (c) as a minimum demonstrates Good Industry Practice;
- (d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
- (e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>);
- (f) takes account of guidance issued by the Centre for Protection of National Infrastructure <https://www.cpni.gov.uk/>
- (g) complies with HMG Information Assurance Maturity Model and Assurance Framework (<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>);
- (h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
- (i) addresses issues of incompatibility with the Supplier's own organisational security policies; and
- (j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph **Error! Reference source not found.**;

19.4.4 document the security incident management processes and incident response plans;

19.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

19.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

19.5 Subject to Paragraph **Error! Reference source not found.** the references to Standards, guidance and policies contained or set out in Paragraph **Error! Reference source not found.** shall be deemed to be references to such items as developed and updated and to any successor

to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

- 19.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph **Error! Reference source not found.**, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
- 19.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 19.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 19 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs **Error! Reference source not found.** to 19.6 shall be deemed to be reasonable.
- 19.8 Approval by the Buyer of the ISMS pursuant to Paragraph 19.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

20 Security Management Plan

- 20.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph **Error! Reference source not found.** fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 20.2.
- 20.2 The Security Management Plan shall:
- 20.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
 - 20.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
 - 20.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
 - 20.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including

the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

20.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

20.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph **Error! Reference source not found.**);

20.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

20.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

20.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

20.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

20.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

20.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 20.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the

Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 20.2 shall be deemed to be reasonable.

- 20.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 20.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

21 Amendment of the ISMS and Security Management Plan

- 21.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:
- 21.1.1 emerging changes in Good Industry Practice;
 - 21.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
 - 21.1.3 any new perceived or changed security threats;
 - 21.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
 - 21.1.5 any new perceived or changed security threats; and
 - 21.1.6 any reasonable change in requirement requested by the Buyer.
- 21.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
- 21.2.1 suggested improvements to the effectiveness of the ISMS;
 - 21.2.2 updates to the risk assessments;
 - 21.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
 - 21.2.4 suggested improvements in measuring the effectiveness of controls.
- 21.3 Subject to Paragraph 21.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 21.1, a Buyer request, a change to Annex **Error! Reference source not found.** (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
- 21.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

22 Security Testing

- 22.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 22.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
- 22.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
- 22.4 Where any Security Test carried out pursuant to Paragraphs 22.2 or 22.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.
- 22.5 If any repeat Security Test carried out pursuant to Paragraph 22.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

23 Complying with the ISMS

- 23.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.
- 23.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.
- 23.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

24 Security Breach

- 24.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.
- 24.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 24.1, the Supplier shall:
- 24.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:
- (a) minimise the extent of actual or potential harm caused by any Breach of Security;
 - (b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
 - (c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

- (d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
- (e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
- (f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

24.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

25 Vulnerabilities and fixing them

25.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

25.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

25.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and

25.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

25.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

25.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

25.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days,

provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

25.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

25.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

25.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

25.4.2 is agreed with the Buyer in writing.

25.5 The Supplier shall:

25.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

25.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

25.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

25.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 19.4.5;

25.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

25.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

25.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

25.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect

the security of the ICT Environment and provide initial indications of possible mitigations.

- 25.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.
- 25.7 A failure to comply with Paragraph 25.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1 Handling Classified information

- 1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2 End user devices

- 2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").
- 2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3 Data Processing, Storage, Management and Destruction

- 3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.
- 3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).
- 3.3 The Supplier shall:
 - 3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
 - 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4 Ensuring secure communications

- 4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.
- 4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5 Security by design

- 5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
- 5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or NCSC certification (<https://www.ncsc.gov.uk/section/products-services/ncsc-certification>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6 Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.
- 6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- 6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
- 6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff

no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7 Restricting and monitoring access

- 7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8 Audit

- 8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
- 8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
 - 8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
- 8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

[REDACTED]

Order Schedule 10 (Exit Management)

9 Definitions

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

"Exclusive Assets"	Supplier Assets used exclusively by the Supplier [or a Key Subcontractor] in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 11.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the DPS Application or Order Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier [or a Key Subcontractor] in connection with the Deliverables but which are also used by the Supplier [or Key Subcontractor] for other purposes;
"Registers"	the register and configuration database referred to in Paragraph 10.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;

"Termination Assistance Notice"	has the meaning given to it in Paragraph 13.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 13.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in Paragraph 16.2.1 of this Schedule;
"Transferring Contracts"	has the meaning given to it in Paragraph 16.2.3 of this Schedule.

10 Supplier must always be prepared for contract exit

- 10.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.
- 10.2 During the Contract Period, the Supplier shall promptly:
 - 10.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and
 - 10.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables ("Registers").
- 10.3 The Supplier shall:
 - 10.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and
 - 10.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify

the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

- 10.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

11 Assisting re-competition for Deliverables

- 11.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").
- 11.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
- 11.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).
- 11.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

12 Exit Plan

- 12.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 12.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.
- 12.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 12.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 12.3 The Exit Plan shall set out, as a minimum:
- 12.3.1 a detailed description of both the transfer and cessation processes, including a timetable;
 - 12.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;
 - 12.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

- 12.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;
- 12.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;
- 12.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;
- 12.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;
- 12.3.8 proposals for the disposal of any redundant Deliverables and materials;
- 12.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and
- 12.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

12.4 The Supplier shall:

12.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

- (a) every [six (6) months] throughout the Contract Period; and
- (b) no later than [twenty (20) Working Days] after a request from the Buyer for an up-to-date copy of the Exit Plan;
- (c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than [ten (10) Working Days] after the date of the Termination Assistance Notice;
- (d) as soon as reasonably possible following, and in any event no later than [twenty (20) Working Days] following, any material change to the Deliverables (including all changes under the Variation Procedure); and

12.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

12.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 12.2 or 12.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

12.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

13 Termination Assistance

13.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

- 13.1.1 the nature of the Termination Assistance required; and
- 13.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the date that the Supplier ceases to provide the Deliverables.
- 13.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than six (6) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.
- 13.3 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph **Error! Reference source not found.**, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

14 Termination Assistance Period

- 14.1 Throughout the Termination Assistance Period the Supplier shall:
 - 14.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;
 - 14.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
 - 14.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
 - 14.1.4 subject to Paragraph 14.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
 - 14.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
 - 14.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
- 14.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 14.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

- 14.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

15 Obligations when the contract is terminated

- 15.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.
- 15.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
- 15.2.1 vacate any Buyer Premises;
 - 15.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;
 - 15.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:
 - (a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and
 - (b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.
- 15.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

16 Assets, Sub-contracts and Software

- 16.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:
- 16.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or
 - 16.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

- 16.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:
- 16.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");
- 16.2.2 which, if any, of:
- (a) the Exclusive Assets that are not Transferable Assets; and
 - (b) the Non-Exclusive Assets,
- the Buyer and/or the Replacement Supplier requires the continued use of; and
- 16.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the "**Transferring Contracts**"),
- in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.
- 16.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.
- 16.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
- 16.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
- 16.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
- 16.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
- 16.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
- 16.7 The Buyer shall:
- 16.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
- 16.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and

exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

16.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

16.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 16.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 16.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

17 No charges

17.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

18 Dividing the bills

18.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

18.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

18.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

18.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

DPS Schedule 7 (Order Procedure and Award Criteria)

Part 1: Order Procedure

Overview

- 1.1. This DPS Schedule sets out the Order Procedure for all Buyers and Suppliers to follow.
- 1.2. CCS reserves the right to change this Order Procedure.
- 1.3. All Buyers listed under the FTS Notice may award an Order Contract under this DPS Contract.
- 1.4. The Buyer may appoint an agent to act on their behalf, this includes completing this Order Procedure.
- 1.5. CCS is not responsible for the actions of any Buyer.

Buyer reserves the right not to award

- 2.1. An Order Procedure may be cancelled at any time. The Buyer is not obliged to award any Order Contract.
- 2.2. At any time during the Further Competition Procedure, the Buyer may go back to any previous stage in the Procedure and amend requirements.
- 2.3. The Supplier may ask clarification questions relating to the Buyer's requirements. The Buyer will specify how clarification questions can be asked and when the clarification period will close. Questions and responses will be anonymised and made available to all Suppliers identified in the Buyer's filtered shortlist as applicable to the Buyer's requirements.

How services will be bought

- 3.1. The Buyer shall award an Order Contract in accordance with the Further Competition Procedure as set out in Clause 4 below.

Further Competition Procedure

- 4.1. **Develop a Statement of Requirements.** The Buyer shall develop a Statement of Requirements detailing what is needed from the Supplier and the outcome that the Supplier shall be required to deliver. As a minimum the Statement of Requirement must include:
 - 4.1.1. an outline of the business challenge/issue, including any known objectives;
 - 4.1.2. details of any mandatory activities, or specialist services that should be included within any proposed solution;

- 4.1.3. the evaluation method and criteria for assessing Suppliers against the Statement of Requirement, based on the Further Competition Award Criteria together with a timetable for the evaluation Procedure;
 - 4.1.4. the number of highest scoring Suppliers that will be invited to Pitch, where applicable, following the Written Proposal; 4.1.5. a request for interested Suppliers to respond; and
 - 4.1.6. the Supplier's Proposal due date.
- 4.2. The Buyer is advised but not mandated to include the below in the Statement of Requirement:
- 4.2.1. a budget range;
 - 4.2.2. geographical location of work (if required);
 - 4.2.3. any security clearances needed;
 - 4.2.4. a clarification period for Suppliers to ask questions about the Statement of Requirements. The time frame for this clarification period shall be outlined in the Statement of Requirements; and
 - 4.2.5. any other information that the Buyer considers necessary to enable Suppliers to submit a Proposal and a template Statement of Requirements layout is attached as Annex A to this Schedule.
- 4.3. The Buyer may wish to engage with Suppliers before starting the below stages, including providing preliminary details of the requirement for Supplier feedback.
- 4.4. The Buyer shall undertake the required stage (clause 4.8 Written Proposal) and may choose to undertake one or more of the optional stages set out below.
- 4.5. **Pre-Market Engagement (Recommended but Optional).** If a Buyer chooses to undertake pre-market engagement the Buyer:
- 4.5.1. shall send the draft Statement of Requirements to all Suppliers on the Buyer's filtered shortlist, as applicable to the Buyer's requirements, asking for a response for the purposes of assisting with market engagement, as detailed within the Statement of Requirements;
 - 4.5.2. may hold a market engagement event where they shall invite all Suppliers on the DPS to help develop the Statement of Requirements; and
 - 4.5.3. may choose to update and re-issue the Statement of Requirements to all Suppliers on the Buyer's filtered shortlist following pre-market engagement.
- 4.6. **Supplier Capability Assessment (Optional).** If a Buyer chooses to undertake Supplier Capability Assessments the Buyer:
- 4.6.1. shall send the Statement of Requirements to all Suppliers on the Buyer's filtered shortlist, as applicable to the Buyer's requirements;

- 4.6.2. shall send questions relating to the requirements set out in the Statement of Requirements to Suppliers which require a “Yes” or “No” response (the “**Capability Assessment Questions**”) and shall indicate the timeframe in which these must be completed.
- 4.6.3. shall only proceed with Suppliers that have responded ‘Yes’ to all the Capability Assessment Questions to the next stage of the Procedure.
- 4.7. Where a Buyer chooses to undertake Supplier capability assessment the Supplier shall respond to the Capability Assessment Questions answering “Yes” or “No”.
- 4.8. **Written Proposal (Required).** The Buyer shall undertake the written Proposal stage for all Order Contracts under this DPS Contract. The Buyer:
- 4.8.1. shall send the Statement of Requirements to all Suppliers on the Buyer’s filtered shortlist, as applicable to the Buyer’s requirements, (or only those Suppliers passing the Capability Assessment if the Buyer has undertaken Supplier Capability Assessment under clause 4.6); and
- 4.8.2. shall conduct a quality and price assessment of the Supplier’s Proposal against the evaluation method and scoring system outlined in the Statement of Requirements.
- 4.9. During the undertaking of the written Proposal stage the Suppliers:
- 4.9.1. shall submit their written Proposal in line with the requirements in the Buyer’s Statement of Requirements including timeframe and format;
- 4.9.2. shall be required to demonstrate how they will deliver the solution, including whether the Services will be delivered solely by their ‘in-house’ capability or whether they intend to SubContract any element(s) of the Services delivering the solution. Where an Supplier declares that it intends to Sub-Contract any element(s) of the Services, the Supplier shall be required to clearly state in its response:
- (a) The name of the Sub-Contractor(s);
 - (b) The Companies House Registration number of the Sub- Contractor(s);
 - (c) The registered address of the Sub-Contractor(s) and the address of the premises from where the Services will be delivered;
 - (d) Details of the Services that will be Sub-Contracted; and
 - (e) the estimated value of the work that will be SubContracted.
- 4.10. **Pre-Pitch Feedback (Recommended when including a pitch but Optional)** The Buyer may choose to undertake a pre-pitch feedback session with each of the Suppliers invited to pitch, to provide feedback on the general direction of the Supplier's approach. These take place before the pitch and are not evaluated.
- 4.11. **Pitch (Recommended but Optional).** If a Buyer chooses to undertake a pitch to further shortlist after the written stage the Buyer shall:

- 4.11.1. specify in the Statement of Requirements that, if the Supplier is successful at the written Proposal stage, that written Proposal must be supported by a further submission in the form of:
 - (a) a presentation;
 - (b) a face to face pitch; or
 - (c) such other submission as the Buyer may specify;
- 4.11.2. specify in the Statement of Requirements how many of the highest scoring Suppliers at the written Proposal stage will be invited to pitch.
- 4.11.3. set out in the Statement of Requirements the evaluation method and scoring system to be used for assessment of the Supplier's further submission; and
- 4.11.4. conduct a quality and price assessment of the Supplier's further submission in line with the evaluation method and scoring system outlined in the Statement of Requirements.
- 4.12. Where a Buyer chooses to undertake a pitch, the Supplier shall address the pitch requirements in its written Proposal.
- 4.13. If the Buyer chooses to undertake a pitching stage, the Supplier shall provide the further submission in accordance with the requirements in the Buyer's Statement of Requirements.
- 4.14. The Buyer shall award an Order Contract to the successful Supplier in accordance with the methodology set out in the Statement of Requirements.
- 4.15. At all stages the Buyer shall notify unsuccessful Suppliers and may provide the Suppliers with feedback.
- 4.16. A Supplier shall inform the Buyer if at any stage it does not wish to participate in the Further Competition Procedure.

Further Competition Award Criteria

- 5.1. The Buyer may wish to use the GCS evaluation framework found here: <https://gcs.civilservice.gov.uk/publications/evaluation-framework/> The Buyer has discretion to develop the Further Competition Award Criteria as it deems appropriate.
- 5.2. The Buyer will evaluate the Supplier's Proposal against the following criteria to determine which of the Suppliers provides the most economically advantageous solution from the perspective of the Buyer. For the avoidance of doubt the most economically advantageous solution will not necessarily be the lowest price solution:

Criteria	Percentage Weightings
Quality*	60 - 95%

Price	5 - 40%
TOTAL	100%

* Central Government Bodies in scope of PPN 06/20 must give Social Value a minimum weighting of 10% of the total scoring

- 5.3. Weightings and sub-weightings for the evaluation criteria will be set by the Buyer and must add up to 100%.
- 5.4. Where the Buyer has chosen to undertake a Pitch, the Buyer will evaluate quality and price in the Written stage to identify Suppliers to invite to Pitch.

What the Supplier has to do

- 6.1. The Supplier agrees that all tenders submitted by the Supplier are made and will be made in good faith and that the Supplier has not fixed or adjusted and will not fix or adjust the price of the tender by or in accordance with any agreement or arrangement with any other person. The Supplier certifies that it has not and undertakes that it will not:
 - 6.1.1. communicate to any person other than the person inviting these tenders the amount or approximate amount of the tender, except where the disclosure, in confidence, of the approximate amount of the tender was necessary to obtain quotations required for the preparation of the tender; and
 - 6.1.2. enter into any arrangement or agreement with any other person that they or the other person(s) shall refrain from submitting a tender or as to the amount of any tenders to be submitted.

Awarding and creating an Order Contract

- 7.1. A Buyer may award an Order Contract with the Supplier by sending (including electronically) a signed Order Form substantially in the form (as may be amended or refined by the Buyer) of the Order Form Template set out in DPS Schedule 6 (Order Form Template and Order Schedules).
- 7.2. The Parties agree that any document or communication (including any document or communication in the apparent form of an Order Contract) which is not as described in this Paragraph 2 shall not constitute an Order Contract under this DPS Contract.
- 7.3. On receipt of an Order Form as described in Paragraph 7.1 from a Buyer the Supplier shall accept the Order Contract by promptly signing and returning (including by electronic means) a copy of the Order Form to the Buyer concerned.
- 7.4. On receipt of the countersigned Order Form from the Supplier, the Buyer shall send (including by electronic means) a written notice of receipt to the Supplier within two

(2) Working Days and the Order Contract shall be formed with effect from the Order Start Date stated in the Order Form.

- 7.5. The Supplier acknowledges that the Buyer is independently responsible for the conduct of its award of Order Contracts under this DPS Contract and that CCS is not responsible or accountable for and shall have no liability whatsoever, except where it is the Buyer, in relation to:

7.5.1. the conduct of Buyer in relation to this Contract; or

7.5.2. the performance or non-performance of any Order Contracts between the Supplier and Buyer entered into pursuant to this Contract.

Awarding and creating an Exempt Order Contract

- 8.1. Paragraph 3.1 above shall not apply to an Exempt Buyer.
- 8.2. If a potential Exempt Buyer decides to source Deliverables through this DPS Contract, it will award an Exempt Order Contract for Deliverables in accordance with the procedure in this Schedule as modified by this Paragraph 8 and in accordance with any legal requirements applicable to that potential Exempt Buyer.
- 8.3. A potential Exempt Buyer may award an Exempt Order Contract under this DPS Contract through a Further Competition Procedure in accordance with Paragraph 4 as modified by Paragraph 8.4 below.
- 8.4. If the potential Exempt Buyer requires the Supplier to develop proposals or a solution in respect of Deliverables, then the potential Exempt Buyer may at its discretion use the procedure set out in Paragraph 4 above as modified by this Paragraph 8.4. In that case, references to “the Regulations” in Paragraph 4 above shall be read as references to “any legal requirements applicable to that potential Exempt Buyer”, and the Exempt Buyer shall be permitted to modify the Further Competition Procedure in accordance with any legal requirements applicable to the Exempt Buyer.
- 8.5. Paragraphs 8.1 to 8.4 above are without prejudice to an Exempt Buyer’s ability to make such further modifications to the Order Procedure as it considers necessary and in accordance with any legal requirements applicable to that potential Exempt Buyer.

Annex A – Template Statement of Requirement

Department / Organisation:

Contact name:

Contact email:

DPS ref:

Date issued / clarification period / response deadline:

Summary

- a) The problem and services required
- b) Any constraints that may preclude Suppliers from accepting this Statement of Requirement
- c) Budget (if appropriate)
- d) Timescales

Context and objectives

- a) About our organisation
- b) Existing strategy (i.e. known sensitivities, constraints, conflicts of interest)
- c) Any data, previous research activity, audience insight and outputs
- d) Your goals and objectives

Requirement and implementation

- a) Detail of requirement
- b) Role of the Supplier, management and staffing (if applicable)
- c) Key delivery milestones

Supplier response (evaluation)

- a) Questions and evaluation methodology with marking scheme
- b) Any further stages

Appointment and timings

- e) Timescales for tender (stages / award)
- f) Contract length and any extension possibilities
- g) Total contract value

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

- 1.1. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 1.2. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
REDACTED	REDACTED	REDACTED	REDACTED

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

- 1.1 The Supplier is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform.
- 1.2 The Supplier is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform who are specifically nominated in the Order Form.
- 1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to the Platform. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
 - 1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 1.3.3 the proposed Key Subcontractor employs unfit persons.
- 1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;
 - 1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - 1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;
 - 1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected DPS Price over the DPS Contract Period;
 - 1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Order Contract Period; and
 - 1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.
- 1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
 - 1.5.1 a copy of the proposed Key Sub-Contract; and
 - 1.5.2 any further information reasonably requested by CCS and/or the Buyer.

- 1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
- 1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - 1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - 1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - 1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - 1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the DPS Contract in respect of:
 - (a) the data protection requirements set out in Clause 14 (Data protection);
 - (b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - (c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
 - (d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - (e) the conduct of audits set out in Clause 6 (Record keeping and reporting);
 - 1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
 - 1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

KEY SUBCONTRACTOR(S)

Key Role	Key Staff	Contact Details
REDACTED	REDACTED	REDACTED

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*);
 - (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 7 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 6 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 6 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 8 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 27 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** Email: **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 2 to paragraph 15 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">• Contact information for the purpose of identifying and facilitating engagement of individuals (specifically, children, parents, non-parents, carers or guardians) in the research.• All personal data collected by the Supplier through interviews, surveys, or workshops as outlined in this annex. <p>A sub-processor is to be engaged by the Supplier and will have access to or process personal data for the duration of the contract. They will be subject to the same conditions as the Supplier as detailed in this agreement.</p>
Duration of the Processing	<p>The duration of the processing of personal and identifiable data collected during the research will last until the completion of the contract, when the final draft report is accepted, and the final payment made. At this point, all identifiable personal information collected during this research must be deleted.</p> <p>Non-identifiable information, such as fully anonymised transcripts can be stored securely for up to seven years after the completion of the contract. At this point all data relating to this contract must be securely deleted.</p>

<p>Nature and purposes of the Processing</p>	<p>The nature of the Processing means any operation required to support research and analysis including: identification of participants, recruitment of participants, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, use, translation, transcription analysis, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means).</p> <p>Processing also includes:</p> <ul style="list-style-type: none"> • disclosure to statutory services such as local authorities, police, NSPCC, Cafcass, Cafcass Cymru, or other statutory bodies • disclosure to support agencies, specifically domestic abuse agencies <p>Where evidence is received that a child or parent is at significant risk of harm or they pose a significant risk of harm to themselves or another. In this instance, the Controller must be notified of the disclosure, but no personal data should be shared with the Controller.</p> <p>Sub-processors are subject to the same conditions as the Supplier as detailed in this agreement.</p> <p><u>Purpose of Processing</u></p> <p>The purpose of processing this data is for research and statistical purposes and for performance of a task carried out in the public interest. This is to support the government in the evaluation of Pathfinder pilots.</p> <p>Personal data processed for research and statistical purposes is done so under the ‘public task’ lawful basis of the UK GDPR. Article 6(1)(e) states:</p> <p>“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”</p> <p>This is supported by section 8 of the Data Protection Act 2018 which states:</p> <p>“personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller’s official authority includes processing of personal data that is necessary for—</p> <p>(a) the administration of justice,</p>
--	---

	<p>(b) the exercise of a function of either House of Parliament,</p> <p>(c) the exercise of a function conferred on a person by an enactment or rule of law,</p> <p>(d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or</p> <p>(e) an activity that supports or promotes democratic engagement.”</p> <p>The MoJ is permitted to process data supplied by the police, the Crown Prosecution Service (CPS), courts and prisons by virtue of its common law powers for the administration of justice. These general powers are supported by various legislative provisions which allow the collection and sharing of information for offender management as well as the establishment and execution of services relevant to the MoJ’s Executive Agencies and ALBs.</p> <p>In addition, where special category data is being processed, this requires a higher level of protection. In order to lawfully process special category data, the MoJ must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. Special category data processed for research and statistical purposes is done so under Article 9(2)(j):</p> <p>“processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.”</p> <p>This is supported by section 4, Part 1 of Schedule 1 of the Data Protection Act 2018.</p> <p>The main use of personal data will be to identify and engage service court users in Pathfinder sites to meet project aims. Specifically, personal identifiable information will be used to:</p> <ul style="list-style-type: none"> • Identify, and screen potential research participants. • Contact and recruit participants for interview or survey. • Facilitate and support participant engagement. • Develop research materials and/or tools. • Conduct and record in-depth interviews, surveys and/or workshops. • Collect, store and manage qualitative and quantitative data. • Analyse research data. • Store processed research data (to include analytical frameworks).
--	--

	<ul style="list-style-type: none"> • Produce interim and final reports and/or presentations. <p>Personal identifiable information used to identify and recruit research participants and those who engage in research (either through interviews, workshops or surveys) should be securely stored by the Supplier. All data collected for research purposes will be destroyed when no longer needed or by the end of the contract.</p>
Type of Personal Data	<p>All personal data collected to complete the commissioned research. This will include a range of personal data about adults and children, such as:</p> <ul style="list-style-type: none"> • Name • Age • Date of birth • Gender • Contact information (email, telephone, address) • Ethnicity, race and/or nationality • Immigration status • Disability or long-term health condition • Sexuality • Place of birth • Children • Parental status • Marital or relationship status (current or previous) • Employment status and nature of employment (including role and workplace) • Wider socio-economic circumstances • Religious or other beliefs • Language • History and experience of family court proceedings • History and experience of criminal proceedings • Personal opinions and experiences • Experience of victimisation and/or harm • Experience of trauma and/or distress • Child's experience of victimisation and/or harm • Child's experience of trauma and/or distress • Child's experience of court process • Perpetration of harm against another (could include: accusations, court findings, criminal convictions) • Support needs • Living situation • Statement of involvement of police / criminal records of themselves or another

	<ul style="list-style-type: none"> • Involvement with children services or other child-centred organisations. • Involvement with other statutory or non-statutory services • Engagement with schools and/or other educational institutions. • Or any other information raised by adults or children during the qualitative interviews.
Categories of Data Subject	<ul style="list-style-type: none"> • Adults including parents, non-parents, carers or guardians who have been involved in private law children's cases in the two Pathfinder courts. • Young people or adults over the age of 16 who were previously subject to private law children's cases in the two Pathfinder courts but are no longer children at the time of the research. • Children below the age of 16 who were subjects of private law children's cases in the two Pathfinder courts. <p>Adults or children may provide additional information on other parties in the proceedings, other professionals involved in the proceedings and potentially other adults or children involved in their life. This could include but is not limited to:</p> <ul style="list-style-type: none"> • Children • Partner or ex-partner • Court and judicial staff • Legal professionals (including lawyers, court advocates). • Cafcass, Cafcass Cymru or local authority staff • Staff providing non-statutory services • Other Family members
<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>Personal identifiable information collected as part of this research must be securely destroyed when no longer required for research purposes, but in any event not later than completion of contract (i.e., when final outputs are accepted by the Authority and final payment is made).</p> <p>Anonymised transcripts, analytical datasets and/or coding frameworks developed for research purposes may be retained for up to seven years following completion of the contract. At this point, all data collected during this contract should be deleted.</p>

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 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 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 Supplier:

- (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 month 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**

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

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.

Order Schedule 4 (Order Tender)

RESPONSE DOCUMENT

REDACTED

Order Schedule 5 (Pricing Details)

REDACTED

Order Schedule 7 (Key Supplier Staff)

- 1.1 The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
 - 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
 - 1.4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 1.5 The Supplier shall:
 - 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
 - 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least three (3) Months’ notice;
 - 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
 - 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

- 1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Annex 1- Key Roles

Key Role		Key Staff		Contact Details	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	
REDACTED		REDACTED		REDACTED	

Order Schedule 14 (Service Levels)

1 Definitions

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Order Form;
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you don't meet the Service Levels

2.1. The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2. The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

2.3. The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4. A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1. the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2. the Service Level Failure:

- (a) exceeds the relevant Service Level Threshold;
- (b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

- (c) results in the corruption or loss of any Government Data; and/or
 - (d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or
- 2.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).
- 2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
 - 2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
 - 2.5..2. the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
 - 2.5..3. there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

- 1.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph **Error! Reference source not found.** shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2 Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

[Guidance Note: The following are included by way of example only. Procurement-specific Service Levels should be incorporated]

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
1. Project proposals (Delivery)	High quality production of research plan, and topic guides and research materials.	MoJ receiving initial project proposals on time as agreed.	Over half of the proposals are delivered late or not delivered at all.	25%
2. Progress reports (Delivery)	Provide progress reports within the agreed format and frequency.	MoJ receiving progress reports fortnightly (unless otherwise mutually agreed to hold at different frequency).	Over half of the progress reports are delivered late or not delivered at all.	10%
3. Project reports and outputs (Delivery)	Provide project reports and outputs	MoJ receiving project reports and outputs on time as agreed.	Report/output delivered > 5 working days after the agreed deadline date and without a robust explanation accepted by MoJ and/or	25%

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
			contains major errors or other significant quality issues which require major re-writing or other intervention by MoJ.	
4. Project reports and outputs (Quality)	Project reports and outputs are of a high quality.	Provision of the reports / outputs.	Report / outputs are not delivered to the agreed standard or require significant rewriting or revisions to be made by MoJ.	30%

The Service Credits shall be calculated on the basis of the following formula:

[Example:

Formula: $x\% \text{ (Service Level Performance Measure)} - x\% \text{ (actual Service Level performance)}$ = $x\% \text{ of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer}$

Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period) = 23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer]

Part B: Performance Monitoring

3 Performance Monitoring and Performance Review

- 3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.
- 3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph **Error! Reference source not found.** of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:
 - 3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
 - 3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;
 - 3.2.3 details of any Critical Service Level Failures;
 - 3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
 - 3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
 - 3.2.6 such other details as the Buyer may reasonably require from time to time.
- 3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
 - 3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;
 - 3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.
- 3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.
- 3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of

the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4 Satisfaction Surveys

- 4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Order Schedule 20 (Order Specification)

Specification Document

Title of Request:	Integrated Domestic Abuse Courts – Pathfinder Pilots Evaluation: Understanding the experience of children and families in Pathfinder
Estimated Total Value:	Between £100-120,000K (excluding VAT)
Duration of Engagement:	10 to 11 months
Required Commencement Date:	February 2024

1. Introduction

This project is being commissioned by the Ministry of Justice (MoJ) Data and Analysis Directorate (DAD). This project is being commissioned through the CCS Research Marketplace Research and Insights Framework ref RM6126.

This specification sets out the requirements for a suitably qualified and experienced contractor to conduct primary research on the experience of children and families who have been through the pathfinder model, to see how their experience aligns with the goals of the Integrated Domestic Abuse Court (IDAC) pilot. The current budget allocated for this research project is £100,000 to £120,000 (exclusive of VAT).

2. Background to the Requirement

In June 2020, the Ministry of Justice published ‘Assessing Risk of Harm to Children and Parents in Private Law Children Cases’¹ (the ‘Harm Panel Report’) which called for widespread reforms to the family court system. It heard evidence that many domestic abuse victims felt like they were being re-traumatised by the current ‘adversarial’ system.

In response to this report, the government committed to pilot a reformed approach to child arrangement proceedings, delivering the 2019 Conservative manifesto commitment to “pilot integrated domestic abuse courts (IDAC) that address criminal and family matters in parallel” and piloting a more investigative approach to the family courts.

As part of the work to achieve this aim to transform how survivors of domestic abuse are treated in family courts, the Ministry of Justice (MoJ) launched the Integrated Domestic Abuse Court (IDAC) pilot to test a more investigative approach to private family law proceedings in Dorset and North Wales. Known as ‘Pathfinders’, these pilots commenced on 21 February 2022 and are currently scheduled to run until 21 February 2024. Through this model, the court will identify families’ needs earlier and work with both adults and children, as well as external agencies like local authorities, the police, and schools, to understand their circumstances and help them to reach an agreement without the need for multiple hearings. A review stage, carried out after an order has been made, will aim to ensure that court orders meet the welfare needs of the child and help to reduce the number of cases that return to court.

The design of the pilots was undertaken by several groups from across the family justice system and related stakeholders. In addition to the Private Law Advisory and Pilots Group (which included members of the judiciary, Cafcass, HCMTS and the Ministry of Justice), stakeholders such as the Family Justice Young People’s Board, academics, police, the Domestic Abuse Commissioner, and charities such as Women’s Aid, Welsh Women’s Aid, Safe Lives, Respect, JUSTICE, Centre for Justice Innovation, and the Nuffield Family Justice Observatory worked on the development of the pilots.

¹ [Assessing Risk of Harm to Children and Parents in Private Law Children Cases \(publishing.service.gov.uk\)](https://publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/904447/Assessing_Risk_of_Harm_to_Children_and_Parents_in_Private_Law_Children_Cases.pdf)

The goals of the pilot are to improve the experiences of children and families by:

- Improving the Family Court experience for all parties, particularly parent victims of domestic abuse and their children; improving children's experience of and (appropriate) participation in the court process.
- Delivering a more efficient court process which reduces delays whilst ensuring that all orders are safe and appropriate to the case.
- Reducing the re-traumatisation of domestic abuse victims, including children, that may be experienced during proceedings.
- Reducing the number of returning cases through a more sustainable court order.
- Adopting a multi-agency approach to improve coordination between the Family Court and agencies, such as local authorities and the police, and the way allegations of domestic abuse and other risks of harm are dealt with.

The pilots were launched on Monday 21 February 2022 in Dorset (Bournemouth and Weymouth), and in North Wales (Caernarfon, Mold, Prestatyn and Wrexham). In these courts, the usual Child Arrangements Process (CAP) has been suspended and replaced with the revised three stage IDAC process for relevant cases. This revision was introduced through the pilot Practice Direction 36Z.²

There are three stages to the new model:

Information Gathering and Assessment - involves a proportionate, child welfare focused approach to actively investigate the impact of issues presented in the application (or any additional information gathered during this phase) on the child. This stage is focused on the development of a Child Impact Report which summarises the issues for the court gathered through engagement with parties, children (where appropriate) and relevant agencies. Domestic abuse support services are engaged to conduct DASH (Domestic Abuse, Stalking and Honour Based Violence) risk assessments³, where appropriate.

Interventions and/or Decision Hearing - following review of the Child Impact Report, the court must then exercise its discretion as to how to enable the application to proceed to a conclusion. This may involve the court recommending the parties pursue non-court resolution, the court ordering further investigation of issues (such as through a fact-finding hearing), the court ordering family interventions (such as periods of supervised contact), or the court being able to make a final order (either by consent or decision of the court).

Review Stage - the final phase of the process is intended to take place 3 to 12 months from the point at which the final order was made, is the review stage. The review is a means of contacting the parties, including children where appropriate, to determine how the order is working for them. The review is focused on the safety of the parties and their children and is used to direct and sign-post families to post-court support. It is not intended to check adherence to court orders, to offer further legal advice or to facilitate complaints about the court process.

This revised process applies to all cases that involve an application for certain section 8 orders or an application for an enforcement order within the pilot courts. All other courts continue to run the CAP. Further details about the process can be found by reviewing the pilot PD (Practice Directions) 36Z.

An update on pilot implementation, following the first year of operation, was published in May 2023 and summarises early findings.⁴ Research is now required to inform decision making about the continuation and rollout of the model, providing evidence of the ways in which the Pathfinder model achieves the core policy goals (outlined above).

MoJ-DAD are commissioning this project to support the evaluation of the Pathfinder courts. The project which is detailed in this specification, will focus on the experience of children and families who have been through

² NEW PRACTICE DIRECTION 36Z - PILOT SCHEME: PRIVATE LAW REFORM: INVESTIGATIVE APPROACH (justice.gov.uk)

³ The Domestic Abuse, Stalking and Honour Based Violence Risk Identification, Assessment and Management Model is a consistent and simple tool for practitioners who work with adult victims of domestic abuse to help them identify those who are at high risk of harm

⁴ Assessing Risk of Harm to Children and Parents in Private Law Children Cases - Annex: Integrated Domestic Abuse Courts (publishing.service.gov.uk)

the Pathfinder model. A second project - a process evaluation and breakeven analysis was commissioned September 2023.

3. Requirement

Research focusing on children's experience of private family law proceedings is limited.⁵ However, there is increasing desire to include the child's voice in research and seek their views on the impact of proceedings on them and their family. Gathering insights from children and families will need to be handled sensitively and with care as appropriate to their age and understanding, to avoid re-traumatisation or distress.

MoJ would like to commission an external research contractor with the necessary skills and experience of private family law to conduct primary research with children and families who have been through the Pathfinder model in Dorset and North Wales.

The contractor will be responsible for delivery of the work by December 2024. They will be responsible for all stages of the research including design, recruitment, fieldwork, analysis, and reporting. The MoJ will have responsibility for decisions on quality threshold, publication, and dissemination of all outputs.

The complexity of this research may require collaboration between two or more organisations and/or individuals with the specialist knowledge to carry out this work. Tenderers should demonstrate they have experience of conducting research with children and families particularly those at risk of or experiencing domestic abuse or harm. Knowledge of the family justice system, in particular private law children's cases is also desirable.

Project aims

The aim of this research is to explore the experience of children and families who have been through the revised Pathfinder model to understand how their experiences align to the key policy goals of IDAC (outlined in Section 2 above).

To address this aim, there are three objectives:

- Objective 1: To understand the lived experience of parents, including parents with experience of or at risk of domestic abuse, who have been an applicant or respondent in a child arrangement case in the Pathfinder courts.
- Objective 2: To understand the lived experience of children and young people, including children and young people with experience of or are at risk of domestic abuse or other harm, who have been subject to a child arrangement application in the Pathfinder courts.
- Objective 3: To explore how the lived experience of children and families relate to the policy goals of IDAC

To respond to this tender, prospective suppliers must provide information on how they will meet the objectives **[Mandatory]**.

We anticipate that the proposed research will involve qualitative interviewing or another suitable qualitative data collection method. However, tenderers can suggest an alternative approach, but they must detail their proposed methods to deliver the requirement, with justification for the approach(es) suggested. **[Mandatory]**.

The following tasks are within scope of the requirement. The Supplier will be required to; **[Mandatory]**

- Design the research. This will include agreeing the final methodological approach to meet research objectives.

⁵ Nuffield Family Justice Observatory (2021) Children's experience of private law proceedings: six key messages from research. Available at: Children's experience of private law proceedings: six key messages from research (nuffieldfjo.org.uk)

- Design the sampling frame and recruitment approach. The contractor will be expected to work with pilot partners to agree access to and recruitment of participants.
- Design qualitative research tools to gather evidence to meet research objectives.
- Conduct the required qualitative fieldwork and analysis gathering insights from children and families.
- Use the data to answer the research objectives and present findings to MoJ through presentations.
- Produce a final report, which subject to clearance and quality assurance, will be published.
- Produce a child-focused output for publication.
- Deliver requirements within agreed timescales.

More details and timings for reporting can be found in [Section 12 Timetable](#).

Knowledge and experience [Mandatory]

- Tenderers must be able to demonstrate a strong background and a proven track record of conducting research with children and families. In particular, conducting research with children and young people at risk of experiencing domestic abuse/ other type of harm and parent victim-survivors of domestic abuse. In addition, knowledge of the family justice system, in particular private law children's cases is desired.
- Tenderers will be expected to provide details of their research team's expertise and experience conducting research with children and families. They will be required to outline how any necessary specialist expertise will be engaged to ensure the research approach is ethically robust. The bid should also include an outline of the skills, experience and the role of any additional experts involved in the project to meet these requirements.
- Contractors are expected to approach this research from a neutral standpoint. The focus should be solely on the voice of the children and families and representing their experience of the pilot.

Engagement of Welsh speakers [Mandatory]

In relation to the evaluation of the project in North Wales, the research provider will need to show how they will comply with HMCTS' Welsh Language Scheme by ensuring that they are:

- a) Aware of the need to provide services through the medium of Welsh and to be sensitive to language choice,
- b) Able to provide Welsh speaking researchers/interviewers if required, and,
- c) Able to provide Welsh or bilingual documentation to an acceptable standard.

In respect of a) and c), HMCTS' Welsh Language Unit may be able to provide assistance if required, but Tenderers should not rely on the MoJ to provide this service.⁶ Tenderers should address this requirement in their bids.

Methods [Mandatory]

- Tenderers must detail their proposed method to deliver the requirement, with justification for the approach(es) suggested. We anticipate that the proposed research approach will consist of a mixture of qualitative research methods appropriately tailored to the needs of the individuals involved.

Engagement with parties [Mandatory]

- We would expect this research to be qualitative in nature and for parties, this may involve some form of either in-depth interviews or focus groups. These could be held face-to-face, by phone, video call or using other means to support engagement (for example, using new digital technologies which offer participants opportunities to be involved in research that is not necessarily face-to-face). Other qualitative methods could be used, and we invite Tenderers to set out their proposed approach and/or methods that they think would best encourage participation of parties with different characteristics,

⁶ HMCTS Welsh language scheme Welsh language scheme - HM Courts & Tribunals Service - GOV.UK (www.gov.uk), paragraphs 12.4, 12.5 and 12.6

experiences and needs (consideration may need to be given to different methods of engaging mothers, fathers and non-parents).

- Tenderers should consider appropriate ways to engage victim-survivors of domestic abuse in this research. This should include proposed methods, with clear justification, and details of mechanisms to ensure both participation and safety.
- Tenderers should outline how they would engage alleged or convicted domestic abuse perpetrators, and those parties alleged or have been found to have caused other forms of harm to their children, safely in this study. Tenders should demonstrate how engagement will be managed to ensure safety and well-being of study participants.

Engagement with children and young people [Mandatory]

- Engagement with children and young people should be designed with their needs in mind. Tenderers should outline their proposed methods and detail how they will facilitate and encourage the participation of children and young people. Tenderers must also demonstrate how they will ensure the safety and well-being of children and young people is maintained throughout and following the end of the project.
- Where possible, we would like this work to capture experiences of children across the age spectrum, using methods that would enable children to participate in their own way and understanding. Tenderers should consider the appropriateness and suitability of methods proposed considering the age and vulnerabilities of the children and young people to be engaged in this work.
- The proposal should also consider when families should be engaged following their involvement in the model.

Access to support [Mandatory]

- Tenderers should outline strategies they intend to use to facilitate and support the participation of families and children in the research. We consider it vital that this research takes an inclusive approach, and that safety and wellbeing is maintained in the research. Strategies could, for example include translators, payment for participation, provision of childcare, the attendance of a support worker, additional support prior and/or following participation, and research materials to best meet the needs of all participants. This list should not be seen as determinative or exhaustive and tenderers are welcome to suggest other approaches to support participant engagement.
- Tenderers must consider how they will support families and children if they become distressed when talking about their experiences. Researchers will need to be attuned to signs of distress and be ready to respond appropriately during engagement. Tenderers will need to consider how they will ensure that re-traumatisation of children and families' is avoided and how they will be supported if the research does cause distress. In their proposal, tenderers will need to outline:
 - how they will manage any episodes of distress and/or disclosure of harm (this could be harm to themselves or possibly to others)
 - what plans are in place to handle any safeguarding concerns.
- Support needs for children are likely differ from those of their parents. Children may be more vulnerable and face different risks than adults. Risks may emerge from the type of questions being asked of them. Tenderers must outline what type of risk may occur as a result of children and families participating in this study and how these may be mitigated. For example, these risks might be mitigated by participants being directed to appropriate child-centred, domestic abuse or mental health support services. We would encourage tenderers to explore other ways any potential risks can be addressed.

- Tenderers may consider it appropriate to support participants to have access to specialist support. It is possible that this could be negotiated with local domestic abuse and family support agencies once the contractor is in post. However, if tenderers feel that any strategies to support families and children can be better addressed by the MoJ, this should be outlined in the tender proposal.

Sampling [Mandatory]

- Tenderers should outline their proposed approach to sampling. This should include:
 - a) proposed sample size (we would like a minimum total of 60 parents and children across the two pilot sites, but tenderers should outline the sample size they think is achievable within the budget and timescale)
 - b) proposed sampling method, and
 - c) key sample criteria.

The proposal should also consider when families should be engaged following their involvement in the model.

- It is expected that a purposive sampling approach will identify families and children that will help answer the objectives outlined in this specification. When designing the sampling criteria, tenderers should look to ensure a diverse sample including:
 - Children (including those affected by domestic abuse and/or other forms of harm, as well as those where no risk of harm was identified in the case)
 - Children who were/were not engaged in proceedings.
 - Parents involved in a case where there is an allegation of domestic abuse (or domestic abuse is a factor in the case)
 - Parents involved in a case where other forms of harm have been raised.
 - Parents involved in a case with no identified element of domestic abuse and/or harm.
- Tenders should seek to ensure a sufficiently robust and diverse sample is weighed against the need to deliver the work within the timescales and budget specified. Whilst we are aiming for a minimum total sample size of 60 parents and children (split across the two pilot sites), we will accept bids with lower sample size if tenderers can outline why this sample is justified.

Participant recruitment [Mandatory]

Tenderers will be:

- Tenderers will be responsible for the recruitment of participants and will need to provide details of how they propose to do this MoJ have engaged Pathfinder operational partners who will work with the supplier to facilitate access to participants', and we expect the successful contractor to work with local pathfinder leads and domestic abuse agencies to identify and recruit participants, with the support of MoJ as and when required.
- MoJ are working with Pathfinder partners to secure approval for the research, but tenderers should expect to complete some additional parts of the research approval process (with the support of MoJ) and build time into their project plan to do so.
- Tenderers should ensure they are able to meet and adhere to the requirements as set out by the pilot partners below.

Requirements for formal approval for research participation [Information]

- Cafcass
<https://www.cafcass.gov.uk/about-cafcass/research/>

- Cafcass Cymru
<https://www.gov.wales/cafcass-cymru>

Cafcass Cymru do not outline a formal research approval process on their website, but MoJ have begun discussions with them on their new process. Tenderers should expect this to be similar in stages and requirements as Cafcass.

- HMCTS
<https://www.gov.uk/guidance/access-hmcts-data-for-research>

Applications will be required to the HCMTS Data Access Panel.

Additional approvals may be required from, for example, Domestic Abuse Support Agencies.

Incentives [Mandatory]

- Recruiting participants willing and able to participate in this type of research may be challenging. Incentives can increase participation levels but also acknowledge the value placed on participants' time and their contribution. In their proposal, tenderers may wish to consider:
 - Whether incentives may be required, and
 - If so, outline their reasons for the use of incentives.
 - Type of incentives they would prefer to use; with children and young people, tenderers may wish to consider what an age-appropriate incentive may look like.
- All costs relating to participation should be included in the proposal. If participants are to be compensated for engagement, the proposal should clearly state the justification for this, as MoJ will need to seek ethical approval for this.
- Approvals for the use of incentives lies with MoJ's Government Social Research Head of Profession and may also be a requirement of pilot partners who support access to participants.

Confidentiality [Mandatory]

- In their proposal, tenderers must outline how they will protect the identity and data relating to children and families approached to take part during the research process. Tenders should outline how information acquired during the research process (and this extends to any measures put in place to safeguard children and families) will be treated in confidence and how this information will be stored and protected.

Phased fieldwork approach [Mandatory]

- We recognise that there are challenges engaging children in research such as this. We expect that the successful contractor may need to work with families/guardians/carers to recruit children to be involved and support their engagement. Time will need to be built into the research to allow time to obtain consent from parents and to support children prior to their involvement. We suggest a phased approach to fieldwork, engaging parents in the first instance as consent is sought to involve children. Tenderers are welcome to suggest an alternative fieldwork approach but will need to outline in full their proposed method.

Tenderers should:

- Ensure that the project team includes those with the skills and experience of working with children and young people. Tenderers should consider how the research can ensure we gain an inclusive insight into the views of all families and children involved in the new pathfinder process.

- Consider how they will ensure that re-traumatisation of families and children are avoided and how they will be supported if the sensitive nature of the research does cause distress.

Analysis [Mandatory]

- The tender should outline their proposed approach to analysing the data collected. Tenderers must outline how they will ensure that the work reflects the experiences of **all participants**, including whether different methods will be required for different participants groups (for example, children).
- The analytical approach will be finalised with MoJ prior to the start of this work.

Project management - Contractor obligations [Mandatory]

- The contractor should nominate a project manager who is the primary contact for the MoJ.
- The contractor will have overall responsibility for management of the research and should ensure that their project manager has sufficient experience, seniority and time allocated to manage the project effectively. They will be responsible for managing the project and ensuring MoJ is kept up to date on project progress.
- It is expected that, following a project inception meeting, regular contact will take place between the tenderer and the MoJ by telephone, email and/or video conferencing meetings. The frequency of contact will be agreed at the project inception meeting. Tenderers should outline how they plan to update MoJ on project progress and how they will communicate emerging findings to the MoJ throughout the project to ensure policy delivery can begin before the research is completed.

Tenderers must:

- Provide a detailed project plan designed to meet the research objectives.
- Identify the project team that will be involved in working on the project, outlining their grade or experience, number of days to be spent on the project, skills, expertise, and nature of their involvement in the research.
- Outline how the contract will be delivered in the event of staff changes during the project.
- Give details of how they will keep the MoJ updated on the progress and emerging findings of the project.
- Describe in detail how they will manage this project to ensure that it runs smoothly.
- Identify risks associated with the successful completion of the research and how they plan to mitigate them.
- Provide details about any sub-contractors or external experts they will be using and for which parts of the project.

Reporting and governance arrangements [Information]

- MoJ-DAD will nominate a contract manager, who will be the successful contractor's first point of contact during the project. They will be responsible for the day-to-day management of the work and manage all administrative issues and contractual and technical matters. They or a nominated replacement will be available to deal with queries.

The contractor:

- Will be expected to engage with the MoJ contract manager proactively throughout the contract to discuss any emerging issues. We should be consulted at all key decision-making stages of the work.
- Will be expected to engage pilot partners in the research design and tenders should outline proposals for doing this.
- Ensure all research instruments and outputs will be sent to the contract manager in the first instance. The contract manager will then be responsible for managing all feedback and for obtaining sign off on final versions.

- Will need to involve the MoJ contract manager in all correspondence between the contractor and wider stakeholders.

Reporting timelines [Mandatory]

The successful contractor will be required to provide the following:

- Draft final report presentation October 2024.
- Draft final report: November 2024
- All agreed final outputs: December 2024

A detailed timeline can be found in Section 11.

Outputs [Mandatory]

The contractor will have responsibility for producing the agreed outputs to an acceptable standard. Tenderers are welcome to suggest additional outputs. It is expected that the outputs from this project will be:

- Up to four presentations to MoJ, pilot partners and/or other family justice stakeholders (for example, on project design, interim findings to support development of final report and final findings with opportunity to discuss implications for pilot operation). Tenderers are welcome to suggest the most appropriate timings for these presentations. Final presentation topics and timings are to be agreed with MoJ once the project is underway.
- Draft final report in November 2024
- Final research report for publication detailing the findings of the research and implications for future pilots This should cover all participants and all research objectives for publication by December 2024
- Final child-focused output for publication by December 2024. Tenderers may wish to consider the most appropriate method of sharing the findings from the research with children (for example, infographics, flow charts)
- Technical research annex outlining the research methods, sampling, and analytical approach (this can be an annex to the final research report or a standalone report) by December 2024.

Quality assurance [Mandatory]

- Tenderers must commit to undertaking quality assurance of all deliverables and to guarantee the accuracy of all outputs. All outputs must be quality assured, including proof reading, before submission to MoJ. MoJ will make the final decision on whether the outputs have met the quality threshold.
- Tenderers must provide details of the quality assurance procedures they have in place in their proposal.
- The research and analysis must adhere to the guidance provided by the HM Treasury Magenta Book.

Risks [Mandatory]

- Tenderers should identify and assess the risks associated with undertaking the research and the proposals for managing and overcoming these. Tenderers must provide a full risk register for all elements of the project.

4. Aims

Recent research has shown what the impact can be on children and young people if they are not listened to. This new approach puts the child at its core, therefore exploring if and how the child has been engaged in Pathfinder proceedings, whether they felt listened and how they felt about their participation in proceedings is essential to understand if the model has been successful in enabling children to engage.

Research is required to understand how the new approach is working from the perspective of children and families. The aim of this research is to explore the experience of children and families who have been through the revised Pathfinder model to understand how their experiences align to the key policy goals of IDAC (Section 2). To address this aim, there are three key objectives.

- Objective 1: To understand the lived experience of parents, including parents with experience of or at risk of domestic abuse, who have been an applicant or respondent in a child arrangement case in the Pathfinder courts.
- Objective 2: To understand the lived experience of children and young people, including children and young people with experience of or are at risk of domestic abuse or other harm, who have been subject to a child arrangement application in the Pathfinder courts.
- Objective 3: To explore how the lived experience of children and families relate to the policy goals of IDAC.

5. Objectives (Measurable Outputs)

The aim of this research is to explore the experience of children and families who have been through the revised Pathfinder model to understand how their experiences align to the key policy goals of IDAC (outlined in Section 2) To address this aim, there are three key objectives:

- Objective 1: To understand the lived experience of parents, including parents with experience of or at risk of domestic abuse, who have been an applicant or respondent in a child arrangement case in the Pathfinder courts.
- Objective 2: To understand the lived experience of children and young people, including children and young people with experience of or are at risk of domestic abuse or other harm, who have been subject to a child arrangement application in the Pathfinder courts.
- Objective 3: To explore how the lived experience of children and families relate to the policy goals of IDAC.

Objective 1:

To understand the lived experience of parents, including parents with experience of or at risk of domestic abuse, who have been an applicant or respondent in a child arrangement case in the Pathfinder courts.

To address objective one, we would expect the research to explore:

- Parent's journeys to make child arrangements in court under the revised Pathfinder model, how parents feel about the revised court process and how it has impacted on themselves and their child(ren). The research should explore parent's experience throughout each of the three stages of the model and explore how parents' cases progressed through the court and what their experiences of each stage were. Families experience of the process of going through family court will differ depending on their specific needs and complexities of their case. Not all user journeys will be the same, and we expect that not all families will have gone through every step of the process.
- Whether the innovative elements introduced within the new approach have affected families' (including children's) experience of proceedings. In particular, we would like to explore parents experience of:

- a) Development of child impact report – including the experience of this more investigative stage of the court process and how parents feel the “front loading” of court work impacted on their case.
 - b) Their child(ren)’s participation in the court process – including how parents feel their child(ren)’s participation (or indeed lack of participation) impacted upon themselves, the court process, and their child(ren).
 - c) Case progression officer – it is hoped that the addition of dedicated CPO (Case Progression Officer) can provide a valuable source of support and advice to families as they navigate an often-complex process. The research should explore parents’ views on their engagement with the CPO and the information provided.
 - d) DASH (Domestic Abuse, Stalking, Harassment) (or equivalent) risk assessments – where cases involve allegations or concerns about domestic abuse, a domestic abuse risk assessment may be carried out. The research should explore parents experience and perception of the use of these risk assessments, including the experience of engagement with the domestic abuse support agency, the experience of completing the DASH and their perceptions on the use of the risk assessment by the court. Where domestic abuse was an issue in the case, but a risk assessment was not carried out, the research should explore the impact of this on a parent’s experience.
 - e) Involvement of IDVAs (Independent Domestic Violence Advisers) and domestic abuse support organisations – where cases involve allegations or concerns about domestic abuse referrals may be made to domestic abuse support agencies. The research should explore parents experience of the support provided by these agencies and how this affected their experience of the court.
 - f) Review stage – where appropriate, the court should order a review in line with the practice direction. Where a review has been completed, the research should explore parents experience of the review, whether they found the review helpful and the impact the review had on them and their child(ren). Where a review was not ordered, the research should explore the impact of this on a parent’s experience. Bidders should note the review stage is usually scheduled between 3 and 12 months after the final order and not all cases will involve a review.
- In cases where there have been allegations or concerns raised about domestic abuse, it is important to understand how parents feel that this has been handled by the courts throughout the process and by all agencies. For example, do parents feel that they have been appropriately supported by agencies (statutory and support agencies) once concerns around domestic abuse or risk of harm have been raised? Consideration should be given to the range of experiences of domestic abuse victims have reported in previous research.
 - Where a court order has been made, tenderers should consider how this decision has impacted on the parents and their child, for example, does the final decision reflect discussions families have had with key agencies, do parents feel their child is happy and safe with the outcome? Tenderers should consider how parents feel allegations of domestic abuse or risk of harm to their children has been addressed by the court and reflected in the outcome.

The Pathfinder process is designed to improve the experience of family courts for some of the most vulnerable users, especially users at risk of domestic abuse. However not all cases will feature domestic abuse. The research will need to capture the lived experience of families involved in cases where there may be other harms or risks (e.g., risks derived from mental health issues, substance misuse) and those cases where there are no “safeguarding” concerns.

Whilst the majority of child arrangement applications are made by separating parents, 10% of private law cases involve other family members or other adults. Grandparent’s account for largest proportion of all non-parents involved in applications but case can be brought not only by direct family members such as aunts

and uncles but also, by foster carers and special guardians. Tenderers should consider how the experiences of non-parents can be captured within this work, if possible.

Objective 2:

To understand the lived experience of children and young people, including children and young people with experience of or are at risk of domestic abuse or other harm, who have been subject to a child arrangement application in Pathfinder courts.

To address objective two, we would like the research to explore:

- How children and young people feel about their experience of being subject to a child arrangement application in the pathfinder courts. The research should consider children's experience of the process, including a specific focus on times when they engaged with the court process/Pathfinder partners as well as their general experiences of being subject to an application.
- Children and young people want to be heard in cases which directly affect them. Existing research shows children and young people want to be told what's happening during proceedings, and have their views heard and believed. Not being listened to can have a negative impact on children and young people adding to what is already a very distressing period in their lives. The research should explore if and how children have been engaged in Pathfinder proceedings, whether they felt listened to and able to influence decisions made and how they feel about their participation in proceedings. This should help to understand whether the model has been successful in enabling children engage appropriately in proceedings.
- This work should also explore how children are listened to and supported throughout proceedings. Children want parents and courts to listen more to their views, but family legal proceedings can be distressing and traumatic for all parties. The research should consider wider questions about the experience of children and the support they were provided with during proceedings.
- Not all children will have been engaged in proceedings, it's equally important to understand this and how this impacted upon their experience of being subject to a child arrangements application in the Pathfinder courts. Tenderers should consider how they can explore the experience of children who have been subject to proceedings, and how being subject to proceedings has affected them.

Objective 3:

To explore how the lived experience of children and families relate to the policy goals of IDAC to see if there is any evidence of the IDAC pilot achieving its purpose.

- To address this objective and deliver the core aim of this research, tenderers will be expected to compare the lived experience of children and families to the core policy goals to explore the extent to which these appear to be met through the pilot. We would expect this strand to be delivered through analysis of the findings from Objectives 1 & 2.
- To help explore the extent to which the policy goals appear to be met through the pilot, tenderers may need to translate the IDAC policy goals into indicators of user experience. These indicators can then be compared to the actual lived experience of children and families to understand whether there is any evidence of the IDAC pilot achieving its core policy goals.
- It will be up to the contractor to determine the best way of doing this. Tenderers should suggest the most appropriate method to achieve this objective, we would particularly welcome approaches that consider a participatory methodology and the involvement of children and families in this strand.
- We do not require the research to attribute any specific impact to the pilot, although tenders are welcome to suggest an impact-based approach if they consider this possible.

Methods

Tenderers must detail their proposed method to deliver the requirement, with justification for the approach(es) suggested. We anticipate that the proposed research approach will consist of a mixture of qualitative research methods appropriately tailored to the needs of the individuals involved.

Outputs

The contractor will have responsibility for producing the agreed outputs to an acceptable standard. Tenderers are welcome to suggest additional outputs. It is expected that the outputs from this project will be:

- Up to four presentations to MoJ, pilot partners and/or other family justice stakeholders (for example, on project design, interim findings to support development of final report and final findings with opportunity to discuss implications for pilot operation). Tenderers are welcome to suggest the most appropriate timings for these presentations. Final presentation topics and timings are to be agreed with MoJ once the project is underway.
- Final research report for publication detailing the findings of the research and implications for future pilots. This should cover all participants and all research objectives for publication by December 2024.
- Final child-focused output for publication by December 2024. Tenderers may wish to consider the most appropriate method of sharing the findings from the research with children (for example, infographics, flow charts)
- Technical research annex outlining the research methods, sampling, and analytical approach (this can be an annex to the final research report or a standalone report) by December 2024.

Final research report

As the final research report is intended for publication, consideration must be given to appropriate communication of complex or emotive findings to a public audience. Research partners should approach drafting from a neutral standpoint. The contractor should provide all written outputs in plain English, and these must be quality assured and proofread before submission to the MoJ.

Technical annex

Transparency is vital and the technical annex should provide a detailed account of the methods used. This can be a separate report or an annex to the main research report and will be published alongside the wider outputs.

Child focused outputs

Content of the child-focused outputs should be handled sensitively, be age appropriate and written in such a way that is understood by children of all ages. Contractors may wish to consider how they engage children in the development of this output.

- The contractor will have responsibility for delivery of listed outputs to the timetable outlined in Section 12 Timetable. All reports will have MoJ branding and will include a disclaimer that the report does not reflect MoJ or government policy and is the opinion of the authors. The reports must conform to the standards set out in MoJ Publications Guidance and must be of an acceptable standard to publish. However, the decision on whether and how the report will be published remains with MoJ.

Structure and format

- Draft reports must be complete including an executive summary, background and policy context, summary of the methods used and detailed description of the key findings. It is expected that the final research reports will be no longer than 25 pages. Further information can be included as annexes which does not count towards the 25-page limit. The technical summary can be as long as is required to outline the approach taken in sufficient detail. The final outputs must be presented in the MoJ format. A template will be provided. The format for the child focused output can be agreed with the successful contractor to ensure it remains accessible to children.

- The content of the final outputs will be agreed with the MoJ. Final research reports must have incorporated feedback from MoJ-DAD, MoJ policy, pilot partners, the GSR Head of Profession and peer reviewers. The designated contract manager at MoJ will be responsible for collating and agreeing feedback from the various parties before passing it on, they will also be responsible for obtaining sign off on final versions. Tenderers should nevertheless indicate how they will engage with pilot partners at the drafting phase. We would suggest tenderers consider early engagement with partners.
- Tenderers should carefully consider the time and resource needed for drafting the final reports, responding to comments, and agreeing final outputs. We cannot outline the number of drafts that will be required at this stage, as this will depend on the quality of outputs. So, contingency should be built into the project plan. We expect Pilot partners will wish to have the opportunity to comment on outputs, therefore, MoJ will require at least ten to twelve working days to comment, review and finalise feedback. Sufficient time must be built into the timeline to allow for this.

6. In Scope, Out of Scope

Included:

Research approval

- The MoJ has secured approval from the President of the Family Division for this project to be considered “approved research” under Practice Direction 12G. This ensures participants can discuss their case with researchers for the purpose of this project.

Ethics

- Tenderers must provide details of all safeguarding and ethical issues relevant to the proposal and how they propose to address these concerns. Tenderers must also provide evidence of how they have successfully addressed similar ethical issues, and secured ethical approval for similar projects, in the past. This should include how appropriate support for the children and families involved might be accessed.
- At a minimum, the research must meet the requirements of the Government Social Researcher (GSR) Professional Guidance: Ethical Assurance for Social Research in Government.
- If tenderers have an ethics board, then their approval must be obtained. We expect this to be a recognised university-based ethics process, or a process that upholds similar standards. If they do not have an ethics board, then ethical approval must be obtained through an independent ethical committee arranged by the successful contactor.
- In advance of the research starting, the successful bidder, MoJ and pilot partners organisations should meet to discuss all ethical issues and the strategies required to ensure the research can be conducted ethically. At this stage, clear lines of responsibility and accountability must be discussed and agreed for all ethical issues.

- We would like the ethical process to be ongoing and expect tenderers to agree to a progressive and shared process of ethical reflection and regular monitoring while the research is taking place. This will ensure that ethical issues are promptly reported to all involved and appropriate advice can be sought if needed. Tenderers should outline their proposal to do this.

Access to support

- Tenderers should outline strategies they intend to use to facilitate and support the participation of families and children and young people in the research. We consider it vital that this research takes an inclusive approach, and that safety and wellbeing is maintained in the research. Strategies could for example, include translators, payment for participation, provision of childcare, the attendance of a support worker, additional support prior and/or following participation, and research materials to best meet the needs of all participants. This list should not be seen as determinative nor exhaustive and tenderers are welcome to suggest other approaches to support participant engagement.
- Tenderers must consider how they will support families and children if they become distressed when talking about their experiences. Researchers will need to be attuned to signs of distress and be ready to respond appropriately during engagement. Tenderers will need to consider how they will ensure that re-traumatisation of children and families' is avoided and how they will be supported if the research does cause distress. In their proposal, tenderers will need to outline:
 - how they will manage any episodes of distress and/or disclosure of harm (this could be harm to themselves or possibly to others)
 - what plans are in place to handle any safeguarding concerns.
- Support needs for children likely differ from those of their parents. Children may be more vulnerable and face different risks than adults. Risks may emerge from the type of questions being asked of them. Tenderers must outline what type of risk may occur as a result of children and families participating in this study and how these may be mitigated. For example, these risks might be mitigated by participants being directed to appropriate child-centred, domestic abuse or mental health support services. We would encourage tenderers to explore of other ways any potential risks can be addressed.
- Tenders may consider it appropriate to support participants to have access to specialist support. It is possible that this could be negotiated with local domestic abuse and family support agencies once the contractor is in post. However, if tenderers feel that any strategies to support families and children can be better addressed by the MoJ, this should be outlined in the tender proposal.

Data Protection

- The successful contractor must comply throughout the project with the MoJ data protection policy and any additional requirements necessary to engage with children and families.
- All data will be collated and stored in accordance with the Data Protection Act 1998, Freedom of Information Act 2000, the General Data Protection Regulation (Regulation (EU) 2016/679) and Government Economic and Social Research Team guidelines - <http://www.civilservice.gov.uk/networks/gsr>.⁷ All published output from the evaluation will be anonymous. The successful contractor must comply throughout the project with the MoJ data protection policy, as set out in Appendix G.
- It is anticipated that the successful contractor will act as a Data Processor on behalf of MoJ. The contractor will be required to store all data in accordance with data protection legislation and current MoJ data security procedures, including Guidance for External Tenderers and Sub-Tenderers working for MoJ using data which is security classified 'Official' or higher.

⁷ See information under GSR Code: Products i.e. legal and ethical subsection.

- The tenderer must ensure all staff working in the project have adequate training in relation to handling data securely and in compliance with the Data Protection Act.
- In addition to the above, the successful contractor must be willing to comply with any reasonable requests in relation to meeting the security requirements of Pilot operational partners if they work to facilities access to participants.
- In their proposal, tenderers must provide details of data protection issues relevant to the proposal and explain how these will be addressed. This should include, how data will be handled and analysed and how they plan to store any personal data, recordings and/or transcripts securely, including retention schedules. The contractor should not share any personal identifiable data with the MoJ.

7. Location of Assignment

Travel to pilot areas – Dorset and North Wales, is likely to be needed to meet pilot partners and to facilitate fieldwork.

Other non-fieldwork and non-engagement research requirements can be delivered remotely.

8. Regulatory requirements

Practice Direction 12G

The MoJ has secured approval from the President of the Family Division for this project to be considered “approved research” under Practice Direction 12G. This ensures participants can discuss their case with researchers for the purpose of this project.⁸

Government Social Researcher Professional Guidance

At a minimum, the research must meet the requirements of the Government Social Researcher (GSR) Professional Guidance: Ethical Assurance for Social Research in Government⁹.

Ethical approval

If tenderers have an ethics board, then their approval must be obtained. We expect this to be a recognised university-based ethics process, or a process that upholds similar standards. If they do not have an ethics board, then ethical approval must be obtained through an independent ethical committee arranged by the successful contactor.

Data Protection

- The successful contractor must comply throughout the project with the MoJ data protection policy and any additional requirements necessary to engage with children and families.
- All data will be collated and stored in accordance with the Data Protection Act 1998, Freedom of Information Act 2000, the General Data Protection Regulation (Regulation (EU) 2016/679) and Government Economic and Social Research Team guidelines - <http://www.civilservice.gov.uk/networks/gsr> . All published output from the evaluation will be

⁸ https://www.justice.gov.uk/courts/procedure-rules/family/practice_directions/pd_part_12g

⁹ <https://www.gov.uk/government/publications/ethical-assurance-guidance-for-social-research-in-government>

anonymous. The successful contractor must comply throughout the project with the MoJ data protection policy.

- It is anticipated that the successful contractor will act as a Data Processor on behalf of MoJ. The contractor will be required to store all data in accordance with data protection legislation and current MoJ data security procedures, including Guidance for External Tenderers and Sub-Tenderers working for MoJ using data which is security classified 'Official' or higher.
- The tenderer must ensure all staff working in the project have adequate training in relation to handling data securely and in compliance with the Data Protection Act.
- In addition to the above, the successful contractor must be willing to comply with any reasonable requests in relation to meeting the security requirements of Pilot operational partners if they work to facilities access to participants.
- In their proposal, tenderers must provide details of data protection issues relevant to the proposal and explain how these will be addressed. This should include, how data will be handled and analysed and how they plan to store any personal data, recordings and/or transcripts securely, including retention schedules. The contractor should not share any personal identifiable data with the MoJ.

Security

- The successful contractor must ensure that all staff working on the project meet Baseline Personnel Security Standard (BPSS) or checks that are equivalent or higher.

9. Service Levels

Contractor requirements

Knowledge and experience

- Tenderers must be able to demonstrate a strong background and a proven track record of conducting research with children and families. In particular, conducting research with children and young people at risk of experiencing domestic abuse/ other type of harm and parent victim-survivors of domestic abuse. In addition, knowledge of the family justice system, in particular private law children's cases is desired.
- We expect tenderers to detail their research team's expertise and experience in conducting research with children and families. They will be required to outline how any necessary specialist expertise will be engaged to ensure the research approach is ethically robust. The bid should also include an outline of the skills, experience and role of any additional experts involved in the project to meet these requirements. Tenderers are required to demonstrate the necessary capacity, available resources, and strong project management skills to deliver the project on time.
- This work is required to inform decision making about the continuation and potential for rollout of the model, providing evidence of the ways in which the Pathfinder model achieves the core policy goals (outlined in Section 2). Potential contractors will need to show they have the relevant research and analytical skills, knowledge of the family justice system and child arrangement proceedings to conduct primary research with children and families.
- Contractors are expected to approach this research from a neutral standpoint. The focus should be solely on the voice of the children and families and representing their experience of the pilot.

Engagement of Welsh Speakers

- In relation to the evaluation of the project in North Wales, the research provider will need to show how they will comply with HMCTS' Welsh Language Scheme by ensuring that they are a) aware of the need to provide services through the medium of Welsh and to be sensitive to language choice b) are able to provide Welsh speaking researchers/interviewers if required and c) are able to provide Welsh or bilingual documentation to an acceptable standard. Tenderers should address this requirement in their bids.

Research approach

- We anticipate that the proposed research approach will consist of a mixture of qualitative research methods appropriately tailored to the needs of the individuals involved. However, tenderers are invited to suggest an alternative approach to deliver the requirement but will need to justify the approaches suggested.

Ethical approval

- Tenderers will be required to detail all safeguarding and ethical issues relevant to the proposal and how they propose to address these concerns. Tenderers will need to provide evidence of how they have successfully addressed similar ethical issues and secured ethical approval for similar projects.

Participant recruitment

- Tenderers will need to provide details on how they intend to recruit participants to gather insights from children and families involved in Pathfinders. We expect the successful contractor to work with local pathfinder leads, pilot partners and local domestic abuse agencies to identify and recruit participants with the support of MoJ as and when is required.

Access to support

- Tenderers will be expected to outline strategies they would put in place to use to facilitate and support the participation of families and children and young people in the research. This research should adopt an inclusive approach is taken, and that safety and wellbeing is maintained in the research. Tenderers are welcome to suggest other approaches to support participant engagement.
- We expect arrangements to be made to support families and children to deal with any distress that may be caused by talking about their experiences. Tenderers should consider how they will ensure that re-traumatisation of children and families' is avoided and how they will be supported if the research does cause distress.

Governance arrangements

- The successful contractor will be expected to proactively engage with the MoJ contract manager for the duration of the work. MoJ should be consulted at all key decision-making stages of the work.
- The contractor will be expected to work closely with MoJ and pilot partners to plan and agree the research design and analysis within the agreed timescales.
- MoJ will be managing all feedback and will be responsible for obtaining agreement and sign off on final versions of the sampling and recruitment approach, use of incentives and data collection tools. The contractor will be required to involve the MoJ contract manager in all correspondence between the contractor and wider stakeholders.

10.KPI's

Social Value Model

As of 1st January 2021, all Central Government contracts are required to deliver Social Value over and above the core deliverable/s of the tender or the contract. All bids will be evaluated under the Social Value Model to determine whether they meet these criteria. The authority places a weighting of 10% of our overall score on how closely suppliers meet our Social Value criteria.

The Social Value Policy Outcome which the bidder must demonstrate is: Improve Health and Wellbeing. As part of your bid, you need to describe the commitment your organisation will make to ensure that opportunities under this contract deliver this Social Value Policy Outcome (see Appendix D for the Model Award Criteria and Sub-Criteria which will be used to assess this policy outcome).

Bidders must include:

- 'Method Statement', stating how they will achieve the Social Value Policy Outcome and how their commitment meets the Award Criteria.
- Timed project plan and process, including how they will implement their commitment and by when. Also, how they will monitor, measure and report on their commitments/the impact of your proposals. Including but not limited to: a timed action plan, use of metrics, tools/processes used to gather data, reporting, feedback and improvement, transparency.

Additional KPIs

Key Performance Indicators						
	KPI	Information needed to measure KPI	How will the KPI be measured?	Red	Amber	Green
1. Project proposals (Delivery)	High quality production of research plan, and topic guides and research materials.	MoJ receiving initial project proposals on time as agreed.	Proposals delivered within the required timescales at the agreed frequency.	Over half of the proposals are delivered late or not delivered at all.	Proposals are mostly on time, but one or more are later than scheduled.	All proposals delivered on time.
2. Progress reports (Delivery)	Provide progress reports within the agreed format and frequency.	MoJ receiving progress reports fortnightly (unless otherwise mutually agreed to hold at different frequency).	Progress reports delivered within the agreed format and frequency.	Over half of the progress reports are delivered late or not delivered at all.	Progress reports are mostly on time, but one or more are later than scheduled.	All progress reports delivered on time.

3. Project reports and outputs (Deliver)	Provide project reports and outputs.	MoJ receiving project reports and outputs on time as agreed.	Project reports and outputs as requested are delivered within the agreed timelines	Report/output delivered > 5 working days after the agreed deadline date and without a robust explanation accepted by MoJ and/or contains major errors or other significant quality issues which require major re-writing or other intervention by MoJ	Report / output delivered up to 5 working days after the deadline date and without a robust explanation accepted by MoJ and/or contains minor errors or other quality issues which require some rewriting or other intervention by MoJ	Meets expectations, reports / outputs are accurate and delivered on time.
4. Project reports and outputs (Quality)	Project reports and outputs are of a high quality.	Provision of the reports / outputs.	Signed off by the Authority's nominated project manager.	Report / outputs are not delivered to the agreed standard or require significant rewriting or revisions to be made by MoJ.	Reports / outputs are delivered but require moderate rewriting and/or revisions to be made by MoJ.	Reports / outputs are delivered to the agreed standard with only minor revisions made by MoJ.
5. Social value – Wellbeing	Effective measures are in place for health and wellbeing of staff.	Health and wellbeing statement / policy / visibility of action plan.	Review of stated policy.	No visible policy or action toward improving workforce health and wellbeing.	Stated policy with no evidenced action.	Evidenced and effective measures with respect to health and wellbeing, including physical and mental health, in the contract workforce.

11. Security arrangements for Consultants

- Baseline Personnel Security Standards (of which Disclosure Scotland is a part) are a default requirement in any Research contract.

<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>

The successful contractor will be required to comply with any reasonable requests from pilot partners for access to their clients. Clear lines of responsibility and accountability should be discussed and agreed prior to the start of the research.

12. Timetable

- We would like all final outputs to be delivered by December 2024. A suggested timeline is outlined below.

Stage	Suggested month of completion 2024
Project initiation meeting	March 2024
Finalise research approach	March 2024
Submission for ethical approval	March 2024
Agree research tools, topics guides and consent forms	March to April 2024
Stakeholder meetings	March 2024
Participant recruitment	May 2024
Fieldwork	May to October 2024
Agreements and/or approvals agreed and signed off	End of June 2024
Analysis	May to November 2024
Interim findings presentation	w/c 15 th or 22 nd July 2024
Co-production workshops	September to October 2024
Final report presentations: MoJ	w/c 28 th October 2024
First draft final report	11 th November 2024
Final report presentations: Key stakeholders	w/c 25 th November 2024
Final report and technical annex	20 th December 2024
Child focused output and policy briefing	w/c 6 th January 2025

- Tenderers are welcome to suggest a modified timetable that would better suit their proposed research. They should ensure this meets the final deadline and outlines all the stages of the research including agreeing the research approach, obtaining ethical approval, fieldwork, and reporting. Tenderers must confirm that they can deliver outputs in accordance with the times set and outline how they will achieve this.

13. Any other Key features

Project costs

Tenderers must submit clear costings for each aspect of the project. This must include a:

- detailed breakdown of what activities each member of the research team will conduct with a specification of the time allocated and their daily rate. A breakdown of the time allocated and day rate for any individuals working on the project.
- Any assumptions associated with the costs (such as research and/or sampling approach, number of participants)
- Total costs
- Costs for project management
- Costs for conducting fieldwork (including recruitment, incentive and participation costs) and analysis
- Costs for reporting
- Costs for transport and subsistence (these should be in line with MoJ guidance)
- Other costs (such as training, translation of research materials, venue hire).

Payment milestones

- Payment milestones will be tied to achievement of key stages of the contract.
- Proposals should include an outline of the proposed payment milestones. A suggestion is given below but tenderers are welcome to propose their own. Please note that proposed payment milestones should be based on project deliverables for the duration of the project.

Milestone and percentage of payment	Milestone	Expected date
REDACTED	Research sign off	May 2024
REDACTED	On completion of 50% of fieldwork	July 2024
REDACTED	On completion of all fieldwork	October 2024
REDACTED	On delivery of the initial draft report	September 2024
REDACTED	On acceptance of all final outputs	December 2024

Response to Tender

The response must be limited to 25 pages of A4 font Arial size 12 (excluding references, footnotes, costing tables and any annexes). The response must include, at a minimum:

- Knowledge:** evidence of understanding of the policy context of the research

- b. **Research approach**: the method(s) and approach(es) that will be used to meet the listed aims and research questions.
- c. **Sampling**: proposed approach to sampling and recruitment
- d. **Engagement**: proposed approach engaging children and families appropriately
- e. **Outputs**: details of proposed outputs including the format and structure of child focused output
- f. **Quality**: details of how quality assurance will be maintained
- g. **Project plan**: a detailed project plan, outlining key stages of the work, designed to meet the research objectives and core delivery dates.
- h. **Project team**: details of the project team that will be involved in working on the project, outlining their experience or grade, number of days on the project, skills, expertise, and nature of their involvement in the research (CVs and supporting information should be included in annexes and are additional to the specified page limit)
- i. **Additional team members**: details of any additional members of the project team who will be sub-contracted or engaged to provide specific expertise to the project; outlining, their background and expertise, number of days on the project, skills, expertise, and nature of their involvement in the research (these are additional to the specified page limit)
- j. **Evidence**: evidence of previous projects, which show experience of delivering similar requirements
- k. **Staff changes**: how the research will be delivered in the event of staff changes during the project
- l. **Project management**: how the contractor will manage the project; including how the contractor will keep MoJ updated on progress and emerging findings throughout the project
- m. **Risk register**: a risk register identifying risks associated with the completion of the research and how tenderers plan to mitigate them.
- n. **Ethics**: details of any ethical issues relevant to the proposal and how these will be addressed, including evidence of how tenderers have managed and successfully obtained ethical approval for similar projects
- o. **Data protection**: details of any data protection issues relevant to the proposal and how these will be addressed; including evidence of how potential contractors have successfully addressed similar ethical issues and received ethical approval for other projects in the past.
- p. **Costs**: clear separate costing for each aspect of the project, including a detailed cost breakdown to be submitted separately from the main proposal.
- q. **Payment schedule**: proposed payment schedule, noting payment is made on deliverables.

Tender evaluation

- Tenders will be evaluated on a value for money basis and quality and social value. More details on the evaluation procedure and criteria can be found in Appendix D - Response Guidance.
- Tenderers should demonstrate they have the necessary experience to deliver the research. This should include.
 - a. Experience of conducting research with children and families, particularly those at risk of or experiencing domestic abuse or harm
 - b. Experience of conducting research that is accessible for children.
 - c. Experience of scoping, designing, and conducting qualitative research
 - d. Writing high quality, succinct reports to a publishable standard
 - e. Strong project management experience, to deliver research to time.

Preferably, tenderers should be able to demonstrate they have.

- f. Knowledge of the family justice system, in particular private law children's cases.
- Tenderers should provide examples in their written response to demonstrate they have the relevant experience. They will also be required to show how they meet the tender evaluation criteria outlined in Appendix D – Response Guidance.

- Once the value for money, price and social value scores for written responses have been finalised, up to 4 tenders will be invited for interview on 19 February 2024. The interview will consist of a 15-minute presentation by the contractor followed by up to 45 minutes of questions. The presentation should include a summary of the proposal including:
 - Proposed approach to conducting the research.
 - Ethical and data protection issues in relation to this project
 - How tenderers will work with the Authority to deliver this work.
- When preparing their presentation, tenderers should assume that both technical and non-technical stakeholders will be on the interview panel.
- The final contractor will be decided based on both the tender and the interview with tender scores for the technical criteria amended following the interview. The successful contractor will be notified soon after the final interview.

14. Outcome

The contractor will have responsibility for producing the agreed outputs to an acceptable standard. Tenderers are welcome to suggest additional outputs. It is expected that the outputs from this project will be:

- Up to four presentations to MoJ, pilot partners and/or other family justice stakeholders (for example, on project design, interim findings to support development of final report and final findings with opportunity to discuss implications for pilot operation). Tenderers are welcome to suggest the most appropriate timings for these presentations. Final presentation topics and timings are to be agreed with MoJ once the project is underway.
- Draft final report in November 2024
- Final research report for publication detailing the findings of the research and implications for future pilots This should cover all participants and all research objectives for publication by December 2024
- Final child-focused output for publication by December 2024. Tenderers may wish to consider the most appropriate method of sharing the findings from the research with children (for example, infographics, flow charts)
- Technical research annex outlining the research methods, sampling, and analytical approach (this can be an annex to the final research report or a standalone report) by December 2024.

The timetable assumes a start date of February 2024. Due to the tight timelines of this project, the successful contractor will be expected to start work on partner engagement and recruitment immediately. This may require some work to begin before contract negotiations are finished.

15. Exit Strategy

Delivery of outputs outlined (Section 14 Outcome) within the required timeline (Section 12 Timetable).