

SHORT FORM CONTRACT FOR THE SUPPLY OF GOODS AND/OR SERVICES**I. Index**

I.	Index.....	1
II.	Cover Letter.....	Error! Bookmark not defined.
III.	Order Form	3
IV.	Short form Terms (“Conditions”)	8
1	Definitions used in the Contract.....	8
2	Understanding the Contract.....	16
3	How the Contract works	17
4	What needs to be delivered	17
5	Pricing and payments	19
6	The Buyer's obligations to the Supplier	20
7	Record keeping and reporting	20
8	Supplier Staff	21
9	Rights and protection.....	22
10	Intellectual Property Rights (“IPRs”)	22
11	Ending the contract.....	24
12	How much you can be held responsible for	26
13	Obeying the Law	27
14	Data Protection and Security	27
15	What you must keep confidential.....	32
16	When you can share information	34
17	Insurance	34
18	Invalid parts of the contract	34
19	Other people's rights in the contract.....	34
20	Circumstances beyond your control	34
21	Relationships created by the contract	35
22	Giving up contract rights.....	35
23	Transferring responsibilities.....	35
24	Supply Chain	35
25	Changing the contract	37
26	How to communicate about the contract	37
27	Dealing with claims	37
28	Preventing fraud, bribery and corruption	37
29	Equality, diversity and human rights.....	38
30	Health and safety.....	38
31	Environment and sustainability.....	39
32	Tax.....	39
33	Conflict of interest	40
34	Reporting a breach of the contract	40
35	Further Assurances	40
36	Resolving disputes.....	40
37	Which law applies	41
V.	Annex 1 – Processing Personal Data.....	42
Part A	Authorised Processing Template.....	42
Part B	Joint Controller Agreement (<i>Optional</i>).....	43
1	Joint Controller Status and Allocation of Responsibilities	Error! Bookmark not defined.

2	Undertakings of both Parties	Error! Bookmark not defined.
3	Data Protection Breach	Error! Bookmark not defined.
4	Audit.....	Error! Bookmark not defined.
5	Impact Assessments.....	Error! Bookmark not defined.
6	ICO Guidance	Error! Bookmark not defined.
7	Liabilities for Data Protection Breach	43
8	Termination.....	44
9	Sub-Processing	44
10	Data Retention.....	45
Part C	Independent Controllers (<i>Optional</i>)	45
1	Independent Controller Provisions	45
VI.	Annex 2 – Specification.....	46
VII.	[Annex 3 – Charges] (<i>Optional</i>)	68
VIII.	[Annex 4 – Supplier Tender] (<i>Optional</i>)	69
IX.	[Annex 5 – Optional IPR Clauses] (<i>Optional</i>)	70
Part A	Buyer ownership with limited Supplier rights to exploit New IPR for the purposes of the current Contract	Error! Bookmark not defined.
10	Intellectual Property Rights (“IPRs”)	Error! Bookmark not defined.
Part B	Supplier ownership of New IPR with Buyer rights for the current Contract and broader public sector functions	Error! Bookmark not defined.
10	Intellectual Property Rights (“IPRs”)	Error! Bookmark not defined.

Order Form

1. Contract Reference	n/a	
2. Buyer	The Department for Work and Pensions (DWP). In entering into this Contract, the Buyer is acting as part of the Crown and the Supplier shall be treated as contracting with the Crown as a whole.	
3. Supplier	RNIB Enterprises Limited, a company registered in England and Wales under company number 00887094 and with registered office at The Grimaldi Building, 154a Pentonville Road, London, N1 9JE.	
4. The Contract	<p>This Contract between the Buyer and the Supplier is for the supply of Deliverables.</p> <p>The Supplier shall supply the Deliverables described below on the terms set out in this Order Form and the attached contract conditions ("Conditions") and Annex 1.</p> <p>Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in the Conditions.</p>	
5. Deliverables	Goods	None
	Services	<p>as set out in Annex 2.</p> <p>The Services are to be performed at:</p> <ul style="list-style-type: none"> • Hub (Yorkshire: Sheffield Kings Court) • Service Centre (Central: Pedmore House) • JCP – Medium (Southern: Worthing Crown House) • JCP – Small (Wales: Pwllheli Lower Cardiff Road) <p>Plus, Quarry House on a call off basis if time allows</p> <p>Date(s) of Delivery: 1 February 2025 to 31 March 2025</p>
6. Specification	The specification of the Deliverables is as set out in Annex 2	
7. Start Date	1 February 2025	
8. Expiry Date	31 March 2025	
9. Extension Period	Not applicable	

10. Buyer Cause	Any Material Breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Buyer is liable to the Supplier.										
11. Optional Intellectual Property Rights ("IPR") Clauses	Not applicable										
12. Charges	<p>The Charges for the Deliverables shall be as set out:</p> <p>The supplier will be paid once DWP confirm the work has been completed.</p> <p>COST BREAKDOWN (EXCLUDING VAT)</p> <table data-bbox="384 864 1497 1245"> <tr> <th data-bbox="384 864 1369 965">Deliverable: Inclusive Design Site Appraisal</th><th data-bbox="1369 864 1497 965">Cost</th></tr> <tr> <td data-bbox="384 965 1369 1043">Hub (Yorkshire)</td><td data-bbox="1369 965 1497 1043"></td></tr> <tr> <td data-bbox="384 1043 1369 1099">Service Centre (Midlands)</td><td data-bbox="1369 1043 1497 1099"></td></tr> <tr> <td data-bbox="384 1099 1369 1155">JCP – Medium (Sussex)</td><td data-bbox="1369 1099 1497 1155"></td></tr> <tr> <td data-bbox="384 1155 1369 1245">JCP – Small (Wales)</td><td data-bbox="1369 1155 1497 1245"></td></tr> </table> <p>_____</p> <p>_____</p>	Deliverable: Inclusive Design Site Appraisal	Cost	Hub (Yorkshire)		Service Centre (Midlands)		JCP – Medium (Sussex)		JCP – Small (Wales)	
Deliverable: Inclusive Design Site Appraisal	Cost										
Hub (Yorkshire)											
Service Centre (Midlands)											
JCP – Medium (Sussex)											
JCP – Small (Wales)											
13. Payment	<p>Payment of undisputed invoices will be made within 30 days of receipt of invoice, which must be submitted promptly by the Supplier.</p> <p>All invoices must be sent, quoting a valid Purchase Order Number (PO Number) and any other relevant details, to:</p> <p>Postal Address</p> <p>Shared Services Connected Limited</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>or</p> <p>Email address _____</p>										

	<p>Within 10 Working Days of receipt of your countersigned copy of this Order Form, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.</p> <p>To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, item number (if applicable) and the details (name, email, and telephone number) of your Buyer contact (i.e. Buyer Authorised Representative). Non-compliant invoices may be sent back to you, which may lead to a delay in payment.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>If you have a query regarding an outstanding payment please contact Shared Services Connected Limited (SSCL), [REDACTED] team by email to: [REDACTED] between 09:00-17:00 Monday to Friday.</p>
<p>14. Data Protection Liability Cap</p>	<p>In accordance with clause 12.6 of the Conditions, the Supplier's total aggregate liability under clause 14.7.5 of the Conditions is no more than the Data Protection Liability Cap, being [REDACTED]</p>
<p>15. Progress Meetings and Progress Reports</p>	<p>Not applicable</p>
<p>16. Buyer Authorised</p>	<p>For general liaison your contacts will continue to be</p>

Representative(s)	<div> <div></div> <div></div> </div>
17. Supplier Authorised Representative(s)	For general liaison your contact will continue to be <div></div>
18. Address for notices	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>
19. Key Staff	Not applicable
20. Procedures and Policies	<p>For the purposes of the Contract the:</p> <p>The Client requires that all Supplier staff employed, whether permanent or temporary, on the provision of the services are subject to the requirements of the HM Government Baseline Personnel Security Standard (BPSS).</p> <p>There is no requirement to apply to the Client or any other third party for BPSS clearance. BPSS clearance is obtained if the following steps have been completed as part of your organisation's pre-employment checks:</p> <ul style="list-style-type: none"> • Verification of identity • Verification of Nationality and Immigration Status (including an entitlement to undertake the work in question) • Verification of Employment history (past 3 years) • Verification of Criminal record (unspent convictions only). This will require a basic disclosure certificate (at cost via Disclosure and Barring Service, Disclosure Scotland and Access Northern Ireland). <p>Copies of the current HM Government Baseline Personnel Security Standard, providing further information regarding how each of these steps should be verified, can be found via the following link Government Baseline Personnel Security Standard. The Supplier is expected to arrange the BPSS checks at no additional charge.</p>

	<p>All personnel must comply with the Client's Security Policy (Annex 2). The Supplier will only be expected to comply with those Security Policies and Standards that are applicable to their delivery model and technologies used.</p> <p>The Supplier must be able to <u>immediately</u> (on contract award) resource this requirement with Supplier personnel meeting the requirements of this section d).</p>
21. Special Terms	The Supplier's indemnities pursuant to clause 12.4 shall be capped [REDACTED]
22. Incorporated Terms	<p>The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies:</p> <ul style="list-style-type: none"> (a) The cover letter from the Buyer to the Supplier dated 7th February 2025 (b) This Order Form (c) Any Special Terms (see row 21 (Special Terms) in this Order Form) (d) Conditions (as they may be amended by [Annex 5 – Optional IPR Clauses] (Optional)) (e) The following Annexes in equal order of precedence: <ul style="list-style-type: none"> i. Annex 1 – Processing Personal Data ii. Annex 2 - Specification

Signed for and on behalf of the Supplier	Signed for and on behalf of the Buyer acting on behalf of the Crown
Name: [REDACTED]	Name: [REDACTED] [REDACTED]
Date:	Date:
Signature: [REDACTED]	Signature: [REDACTED]

II. Short form Terms (“Conditions”)

1 DEFINITIONS USED IN THE CONTRACT

1.1 In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

“Affiliates”	in relation to a body corporate, any other entity which directly or indirectly Controls (in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and “ Controlled ” shall be construed accordingly), is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
“Audit”	<p>the Buyer’s right to:</p> <ul style="list-style-type: none"> (a) verify the accuracy of the Charges and any other amounts payable by the Buyer under the 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 Deliverables; (c) verify the Supplier’s and each Subcontractor’s compliance with the applicable Law; (d) identify or investigate actual or suspected breach of clauses 4 to 34 (inclusive), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Buyer shall have no obligation to inform the Supplier of the purpose or objective of its investigations; (e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any Subcontractors or their ability to provide the Deliverables; (f) obtain such information as is necessary to fulfil the Buyer’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; (g) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Contract; (h) carry out the Buyer’s internal and statutory audits and to prepare, examine and/or certify the Buyer’s annual and interim reports and accounts; (i) 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 Buyer has used its resources;

“Beneficiary”	A Party having (or claiming to have) the benefit of an indemnity under this Contract;
“Buyer Cause”	has the meaning given to it in the Order Form;
“Buyer”	the person named as Buyer in the Order Form. Where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole;
“Charges”	the charges for the Deliverables as specified in the Order Form;
“Claim”	any claim which it appears that the Buyer is, or may become, entitled to indemnification under this Contract;
“Conditions”	means these short form terms and conditions of contract;
“Confidential Information”	all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which <ul style="list-style-type: none"> (a) is known by the receiving Party to be confidential; (b) is marked as or stated to be confidential; or (c) ought reasonably to be considered by the receiving Party 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 the Buyer under the Contract, in the reasonable opinion of the Buyer;
“Contract”	the contract between the Buyer and the Supplier which is created by the Supplier’s counter signing the Order Form and includes the cover letter (if used), Order Form, these Conditions and the Annexes;
“Controller”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Crown Body”	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), 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;
“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;

“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”	<ul style="list-style-type: none"> (a) the UK GDPR, (b) the DPA 2018; (c) all applicable Law about the processing of personal data and privacy and guidance issued by the Information Commissioner and other regulatory authority; and (d) (to the extent that it applies) the EU GDPR (and in the event of conflict, the UK GDPR shall apply);
“Data Protection Liability Cap”	has the meaning given to it in row 14 of the Order Form;
“Data Protection Officer”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“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;
“Data Subject”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Deliver”	hand over of the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and stacking and any other specific arrangements agreed in accordance with clause 4.2. “Delivered” and “Delivery” shall be construed accordingly;
“Deliverables”	means the Goods, Services, and/or software to be supplied under the Contract as set out in the Order Form;
“DPA 2018”	the Data Protection Act 2018;
“EU GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
“Existing IPR”	any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise);
“Expiry Date”	the date for expiry of the Contract as set out in the Order Form;

“FOIA”	the Freedom of Information Act 2000 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, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from:</p> <ul style="list-style-type: none"> (a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Party seeking to claim relief in respect of a Force Majeure Event (the “Affected Party”) which prevent or materially delay the Affected Party from performing its obligations under the Contract; (b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; (c) acts of a Crown Body, local government or regulatory bodies; (d) fire, flood or any disaster; or (e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available <p>but excluding:</p> <ul style="list-style-type: none"> (a) 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; (b) 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; and (c) any failure of delay caused by a lack of funds, <p>and which is not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party;</p>
“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;
“Goods”	the goods to be supplied by the Supplier to the Buyer under the Contract;
“Government Data”	<ul style="list-style-type: none"> (a) 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 Buyer's confidential information, and which: <ul style="list-style-type: none"> (i) are supplied to the Supplier by or on behalf of the Buyer; or

	<p>(ii) the Supplier is required to generate, process, store or transmit pursuant to the Contract; or</p> <p>(b) any Personal Data for which the Buyer is the Controller;</p>
“Indemnifier”	a Party from whom an indemnity is sought under this Contract;
“Independent Controller”	a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data;
“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;
“Insolvency Event”	<p>in respect of a person:</p> <p>(a) if that person is insolvent;</p> <p>(b) where that person is a company, LLP or a partnership, if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction);</p> <p>(c) if an administrator or administrative receiver is appointed in respect of the whole or any part of the person’s assets or business;</p> <p>(d) if the person makes any composition with its creditors; or</p> <p>(e) takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction;</p>
“IP Completion Day”	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;
“Joint Controller Agreement”	the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Part B Joint Controller Agreement (<i>Optional</i>) of Annex 1 – Processing Personal Data;
“Joint Controllers”	Where two or more Controllers jointly determine the purposes and means of processing;
“Key Staff”	any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier;
“Law”	any law, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of

	practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
“Material Breach”	a single serious breach or a number of breaches or repeated breaches (whether of the same or different obligations and regardless of whether such breaches are remedied)
“National Insurance”	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
“New IPR Items”	means a deliverable, document, product or other item within which New IPR subsists;
“New IPR”	all and intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Contract but shall not include the Supplier's Existing IPR;
“Open Licence”	means any material that is published for use, with rights to access and modify, by any person for free, under a generally recognised open licence including Open Government Licence as set out at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ as updated from time to time and the Open Standards Principles documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles as updated from time to time;
“Order Form”	the order form signed by the Buyer and the Supplier printed above these Conditions;
“Party”	the Supplier or the Buyer (as appropriate) and “Parties” shall mean both of them;
“Personal Data Breach”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires and includes any breach of Data Protection Legislation relevant to Personal Data processed pursuant to the Contract;
“Personal Data”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“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 as updated from time to time;

“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 the Contract;
“Processor”	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
“Protective Measures”	<p>technical and organisational measures which must take account of:</p> <ul style="list-style-type: none"> (a) the nature of the data to be protected; (b) harm that might result from Data Loss Event; (c) state of technological development; (d) the cost of implementing any measures; <p>including 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;</p>
“Purchase Order Number” or “PO Number”	the Buyer’s unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the Contract;
“Rectification Plan”	<p>the Supplier’s plan (or revised plan) to rectify its Material Breach which shall include:</p> <ul style="list-style-type: none"> (a) full details of the Material Breach that has occurred, including a root cause analysis; (b) the actual or anticipated effect of the Material Breach; and (c) the steps which the Supplier proposes to take to rectify the Material Breach (if applicable) and to prevent such Material Breach from recurring, including timescales for such steps and for the rectification of the Material Breach (where applicable);
“Regulations”	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time;
“Request For Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Services”	the services to be supplied by the Supplier to the Buyer under the Contract;
“Specification”	the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form;

“Staff Vetting Procedures”	vetting procedures that accord with Good Industry Practice or, where applicable, the Buyer’s procedures or policies for the vetting of personnel as specified in the Order Form or provided to the Supplier in writing following agreement to the same by the Supplier from time to time;
“Start Date”	the start date of the Contract set out in the Order Form;
“Sub-Contract”	any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party: <ul style="list-style-type: none"> (a) provides the Deliverables (or any part of them); (b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or (c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
“Subcontractor”	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
“Subprocessor”	any third party appointed to process Personal Data on behalf of the Processor related to the Contract;
“Supplier Staff”	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier’s obligations under the Contract;
“Supplier”	the person named as Supplier in the Order Form;
“Term”	the period from the Start Date to the Expiry Date as such period may be extended in accordance with clause 11.2 or terminated in accordance with the Contract;
“Third Party IPR”	intellectual property rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
“Transparency Information”	<p>In relation to Contracts with a value above the relevant threshold set out in Part 2 of the Regulations only, the content of the Contract, including any changes to this Contract agreed from time to time, as well as any information relating to the Deliverables and performance pursuant to the Contract required to be published by the Buyer to comply with its transparency obligations, including those set out in Public Procurement Policy Note 09/21 (update to legal and policy requirements to publish procurement information on Contracts Finder)</p> <p>(https://www.gov.uk/government/publications/ppn-0921-requirements-to-publish-on-contracts-finder) as updated from time to time and Public Procurement Policy Note 01/17 (update to transparency principles) where applicable</p> <p>(https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles) as updated from time to time except for:</p>

	(a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Buyer; and (b) Confidential Information;
“UK GDPR”	has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4);
“VAT”	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
“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) as updated from time to time applies in respect of the Deliverables; and
“Working Day”	a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

2 UNDERSTANDING THE CONTRACT

2.1 In the Contract, unless the context otherwise requires:

- 2.1.1 references to numbered clauses are references to the relevant clause in these Conditions;
- 2.1.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
- 2.1.3 references to “writing” include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;
- 2.1.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated, replaced or re-enacted from time to time (including as a consequence of the Retained EU Law (Revocation and Reform) Act) and to any legislation or byelaw made under that Law;
- 2.1.5 the word “including”, “for example” and similar words shall be understood as if they were immediately followed by the words “without limitation”;

- 2.1.6 any reference which, immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to section 1A of the European Union (Withdrawal) Act 2018), is a reference to (as it has effect from time to time) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 and which shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time.

3 HOW THE CONTRACT WORKS

- 3.1 The Order Form is an offer by the Buyer to purchase the Deliverables subject to and in accordance with the terms and conditions of the Contract.
- 3.2 The Supplier is deemed to accept the offer in the Order Form when the Buyer receives a copy of the Order Form signed by the Supplier.
- 3.3 The Supplier warrants and represents that its tender (if any) and all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

4 WHAT NEEDS TO BE DELIVERED

4.1 All Deliverables

- 4.1.1 The Supplier must provide Deliverables:
- 4.1.1.1 in accordance with the Specification, (where applicable) and the Contract;
 - 4.1.1.2 using reasonable skill and care;
 - 4.1.1.3 using Good Industry Practice;
 - 4.1.1.4 using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract;
 - 4.1.1.5 on the dates agreed; and
 - 4.1.1.6 that comply with all Law.
- 4.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days (or longer where the Supplier offers a longer warranty period to its Buyers) from Delivery against all obvious defects.

4.2 Goods clauses

- 4.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.
- 4.2.2 The Supplier transfers ownership of the Goods on completion of Delivery or payment for those Goods, whichever is earlier.
- 4.2.3 Risk in the Goods transfers to the Buyer on Delivery, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

- 4.2.4 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.
- 4.2.5 The Supplier must Deliver the Goods on the date and to the location specified in the Order Form, during the Buyer's working hours (unless otherwise specified in the Order Form).
- 4.2.6 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.
- 4.2.7 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.
- 4.2.8 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.
- 4.2.9 The Supplier will notify the Buyer of any request that Goods are returned to it or the manufacturer after the discovery of safety issues or defects that might endanger health or hinder performance and shall indemnify the Buyer against the costs arising as a result of any such request.
- 4.2.10 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable endeavours to minimise these costs.
- 4.2.11 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with clause 4.2. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.
- 4.2.12 The Buyer will not be liable for any actions, claims, costs and expenses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Buyer or its servant or agent. If the Buyer suffers or incurs any damage or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Buyer from any losses, charges, costs or expenses which arise as a result of or in connection with such damage or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Staff.

4.3 Services clauses

- 4.3.1 Late Delivery of the Services will be a default of the Contract.
- 4.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions including the security requirements (where any such requirements have been provided).
- 4.3.3 The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services

- 4.3.4 The Supplier must at its own risk and expense provide all equipment required to deliver the Services. Any equipment provided by the Buyer to the Supplier for supplying the Services remains the property of the Buyer and is to be returned to the Buyer on expiry or termination of the Contract.
- 4.3.5 The Supplier must allocate sufficient resources and appropriate expertise to the Contract.
- 4.3.6 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
- 4.3.7 On completion of the Services, the Supplier is responsible for leaving the Buyer's premises in a clean, safe and tidy condition and making good any damage that it has caused to the Buyer's premises or property, other than fair wear and tear.
- 4.3.8 The Supplier must ensure all Services, and anything used to deliver the Services, are of good quality and free from defects.
- 4.3.9 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

5 PRICING AND PAYMENTS

- 5.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the charges in the Order Form.
- 5.2 All Charges:
 - 5.2.1 exclude VAT, which is payable on provision of a valid VAT invoice; and
 - 5.2.2 include all costs and expenses connected with the supply of Deliverables.
- 5.3 The Buyer must pay the Supplier the charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds to the Supplier's account stated in the invoice or in the Order Form.
- 5.4 A Supplier invoice is only valid if it:
 - 5.4.1 includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer; and
 - 5.4.2 includes a detailed breakdown of Deliverables which have been delivered.
- 5.5 If there is a dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 36.
- 5.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier under this Contract or any other agreement between the Supplier and the Buyer if notice and reasons are provided.

- 5.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, the Buyer can publish the details of the late payment or non-payment.

6 THE BUYER'S OBLIGATIONS TO THE SUPPLIER

- 6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:
- 6.1.1 the Buyer cannot terminate the Contract under clause 11;
 - 6.1.2 the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;
 - 6.1.3 the Supplier is entitled to additional time needed to deliver the Deliverables; and
 - 6.1.4 the Supplier cannot suspend the ongoing supply of Deliverables.
- 6.2 Clause 6.1 only applies if the Supplier:
- 6.2.1 gives notice to the Buyer within 10 Working Days of becoming aware;
 - 6.2.2 demonstrates that the failure only happened because of the Buyer Cause; and
 - 6.2.3 mitigated the impact of the Buyer Cause.

7 RECORD KEEPING AND REPORTING

- 7.1 The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in the Order Form.
- 7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the date of expiry or termination of the Contract and in accordance with the UK GDPR or the EU GDPR as the context requires.
- 7.3 The Supplier must allow any auditor appointed by the Buyer access to its premises to verify all contract accounts and records of everything to do with the Contract and provide copies for the Audit.
- 7.4 The Buyer or an auditor can Audit the Supplier.
- 7.5 During an Audit, the Supplier must provide information to the auditor and reasonable co-operation at their request.
- 7.6 The Parties will bear their own costs when an Audit is undertaken unless the Audit identifies a Material Breach by the Supplier, in which case the Supplier will repay the Buyer's reasonable costs in connection with the Audit.
- 7.7 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:
- 7.7.1 tell the Buyer and give reasons;
 - 7.7.2 propose corrective action; and
 - 7.7.3 provide a deadline for completing the corrective action.

- 7.8 If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Contract then the Buyer may:
- 7.8.1 require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand; and
 - 7.8.2 if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Contract immediately for Material Breach (or on such date as the Buyer notifies) and the consequences of termination in Clause 11.5.1 shall apply.
- 7.9 If there is a Material Breach, the Supplier must notify the Buyer within 3 Working Days of the Supplier becoming aware of the Material Breach. The Buyer may request that the Supplier provide a Rectification Plan within 10 Working Days of the Buyer's request alongside any additional documentation that the Buyer requires. Once such Rectification Plan is agreed between the Parties (without the Buyer limiting its rights) the Supplier must immediately start work on the actions in the Rectification Plan at its own cost.

8 SUPPLIER STAFF

- 8.1 The Supplier Staff involved in the performance of the Contract must:
- 8.1.1 be appropriately trained and qualified;
 - 8.1.2 be vetted in accordance with the Staff Vetting Procedures; and
 - 8.1.3 comply with all conduct requirements when on the Buyer's premises.
- 8.2 Where the Buyer decides one of the Supplier's Staff isn't suitable to work on the Contract, the Supplier must replace them with a suitably qualified alternative.
- 8.3 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.
- 8.4 The Supplier indemnifies the Buyer against all claims brought by any person employed or engaged by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.
- 8.5 The Buyer indemnifies the Supplier against all claims brought by any person employed or engaged by the Buyer caused by an act or omission of the Buyer or any of the Buyer's employees, agents, consultants and contractors.
- 8.6 The Supplier shall use those persons nominated (if any) as Key Staff in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier to provide the Deliverables and shall not remove or replace any of them unless:
- 8.6.1 requested to do so by the Buyer or the Buyer approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 8.6.2 the person concerned resigns, retires or dies or is on parental or long-term sick leave; or

8.6.3 the person's employment or contractual arrangement with the Supplier or any Subcontractor is terminated for material breach of contract by the employee.

8.7 The Supplier shall ensure that no person who discloses that they have a conviction that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a “**Relevant Conviction**”), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a disclosure and barring service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

9 RIGHTS AND PROTECTION

9.1 The Supplier warrants and represents that:

- 9.1.1 it has full capacity and authority to enter into and to perform the Contract;
- 9.1.2 the Contract is entered into by its authorised representative;
- 9.1.3 it is a legally valid and existing organisation incorporated in the place it was formed;
- 9.1.4 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;
- 9.1.5 all necessary rights, authorisations, licences and consents (including in relation to IPRs) are in place to enable the Supplier to perform its obligations under the Contract and the Buyer to receive the Deliverables;
- 9.1.6 it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and
- 9.1.7 it is not impacted by an Insolvency Event.

9.2 The warranties and representations in clause 3.3 and clause 9.1 are repeated each time the Supplier provides Deliverables under the Contract.

9.3 The Supplier indemnifies the Buyer against each of the following:

- 9.3.1 wilful misconduct of the Supplier, any of its Subcontractor and/or Supplier Staff that impacts the Contract; and
- 9.3.2 non-payment by the Supplier of any tax or National Insurance.

9.4 If the Supplier becomes aware of a representation or warranty made in relation to the Contract that becomes untrue or misleading, it must immediately notify the Buyer.

9.5 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier for free.

10 INTELLECTUAL PROPERTY RIGHTS (“IPRS”)

10.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable, sub-licensable worldwide licence to use, copy and adapt the Supplier's Existing IPR to enable the Buyer and its sub-licensees to both:

- 10.1.1 receive and use the Deliverables; and

10.1.2 use the New IPR.

The termination or expiry of the Contract does not terminate any licence granted under this clause 10.

- 10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs and the New IPR which the Supplier reasonably requires for the purpose of fulfilling its obligations during the Term and commercially exploiting the New IPR developed under the Contract. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).
- 10.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.
- 10.4 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract, it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.
- 10.5 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this clause 10 or otherwise agreed in writing.
- 10.6 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.
- 10.7 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:
- 10.7.1 obtain for the Buyer the rights in clause 10.1 without infringing any third party intellectual property rights; and
 - 10.7.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.
 - 10.7.3 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clauses 11.5.1 shall apply.
- 10.8 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:
- 10.8.1 the Buyer gives its approval to do so; and
 - 10.8.2 one of the following conditions applies:
 - 10.8.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 10.1; or

- 10.8.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 10.8.2.1:
- (a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;
 - (b) the Buyer agrees to those licence terms; and
 - (c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or
- 10.8.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

10.9 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it, does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.

11 ENDING THE CONTRACT

- 11.1 The Contract takes effect on the Start Date and ends on the earlier of the Expiry Date or termination of the Contract, or earlier if required by Law.
- 11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form.
- 11.3 **Ending the Contract without a reason**
- 11.3.1 The Buyer has the right to terminate the Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice, and if it's terminated clause 11.6.2 applies.

11.4 When the Buyer can end the Contract

- 11.4.1 If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier and the consequences of termination in Clause 11.5.1 shall apply:
- 11.4.1.1 there's a Supplier Insolvency Event;
 - 11.4.1.2 the Supplier is in Material Breach of the Contract;
 - 11.4.1.3 there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which isn't pre-approved by the Buyer in writing;
 - 11.4.1.4 the Buyer discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded;
 - 11.4.1.5 the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them; or

11.4.1.6 the Supplier fails to comply with its legal obligations in the fields of environmental, social, equality or employment Law when providing the Deliverables.

11.4.2 If any of the events in 73(1) (a) or (b) of the Regulations happen, the Buyer has the right to immediately terminate the Contract and clauses 11.5.1.2 to 11.5.1.7 apply.

11.5 What happens if the Contract ends

11.5.1 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 39 of Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data (if used), all of the following apply:

11.5.1.1 the Supplier is responsible for the Buyer's reasonable costs of procuring replacement Deliverables for the rest of the term of the Contract;

11.5.1.2 the Buyer's payment obligations under the terminated Contract stop immediately;

11.5.1.3 accumulated rights of the Parties are not affected;

11.5.1.4 the Supplier must promptly delete or return the Government Data except where required to retain copies by Law;

11.5.1.5 the Supplier must promptly return any of the Buyer's property provided under the Contract;

11.5.1.6 the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer and any incoming supplier and co-operate fully in the handover and re-procurement; and

11.5.1.7 the Supplier must repay to the Buyer all the Charges that it has been paid in advance for Deliverables that it has not provided as at the date of termination or expiry.

11.5.2 The following clauses survive the expiry or termination of the Contract: 1, 4.2.9, 5, 7, 8.4, 10, 11.5, 12, 14, 15, 16, 18, 19, 32.2.2, 36 and 37 and any clauses which are expressly or by implication intended to continue.

11.6 When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination)

11.6.1 The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.

11.6.2 Where the Buyer terminates the Contract in accordance with clause 11.3 or the Supplier terminates the Contract under clause 11.6 or 23.4:

11.6.2.1 the Buyer must promptly pay all outstanding charges incurred by the Supplier;

11.6.2.2 the Buyer must pay the Supplier reasonable committed and unavoidable losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated; and

11.6.2.3 clauses 11.5.1.2 to 11.5.1.7 apply.

11.6.3 The Supplier also has the right to terminate the Contract in accordance with Clauses 20.3 and 23.4.

11.7 Partially ending and suspending the Contract

11.7.1 Where the Buyer has the right to terminate the Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Contract it can provide the Deliverables itself or buy them from a third party.

11.7.2 The Buyer can only partially terminate or suspend the Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.

11.7.3 The Parties must agree (in accordance with clause 25) any necessary variation required by clause 11.7, but the Supplier may not either:

11.7.3.1 reject the variation; or

11.7.3.2 increase the Charges, except where the right to partial termination is under clause 11.3.

11.7.4 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.7.

12 HOW MUCH YOU CAN BE HELD RESPONSIBLE FOR

12.1 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than 125% of the Charges paid or payable to the Supplier.

12.2 No Party is liable to the other for:

12.2.1 any indirect losses; and/or

12.2.2 loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

12.3 In spite of clause 12.1, neither Party limits or excludes any of the following:

12.3.1 its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;

12.3.2 its liability for bribery or fraud or fraudulent misrepresentation by it or its employees; or

12.3.3 any liability that cannot be excluded or limited by Law.

12.4 In spite of clause 12.1, the Supplier does not limit or exclude its liability for any indemnity given under clauses 8.4, 9.3.2, 10.6, or 32.2.2.

12.5 In spite of clause 12.1, the Buyer does not limit or exclude its liability for any indemnity given under clause 8.5.

- 12.6 Notwithstanding clause 12.1, but subject to clauses 12.1 and 12.3, the Supplier's total aggregate liability under clause 14.7.5 shall not exceed the Data Protection Liability Cap.
- 12.7 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.
- 12.8 If more than one Supplier is party to the Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

13 OBEYING THE LAW

- 13.1 The Supplier, in connection with provision of the Deliverables:
- 13.1.1 is expected to meet and have its Subcontractors meet the standards set out in the Supplier Code of Conduct:
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier Code of Conduct v3.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdf) as such Code of Conduct may be updated from time to time, and such other sustainability requirements as set out in the Order Form. The Buyer also expects to meet this Code of Conduct;
 - 13.1.2 must comply with the provisions of the Official Secrets Acts 1911 to 1989 and section 182 of the Finance Act 1989;
 - 13.1.3 must support the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010;
 - 13.1.4 must comply with the model contract terms contained in (a) to (m) of Annex C of the guidance to [PPN 02/23 \(Tackling Modern Slavery in Government Supply Chains\)](https://www.gov.uk/government/publications/ppn-0223-tackling-modern-slavery-in-government-supply-chains),¹ as such clauses may be amended or updated from time to time; and
 - 13.1.5 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>, as updated from time to time.
- 13.2 The Supplier indemnifies the Buyer against any costs resulting from any default by the Supplier relating to any applicable Law to do with the Contract.
- 13.3 The Supplier must appoint a compliance officer who must be responsible for ensuring that the Supplier complies with Law, clause 13.1 and clauses 27 to 34.

14 DATA PROTECTION AND SECURITY

- 14.1 The Supplier must not remove any ownership or security notices in or relating to the Government Data.
- 14.2 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies via secure encrypted method upon reasonable request.

¹ <https://www.gov.uk/government/publications/ppn-0223-tackling-modern-slavery-in-government-supply-chains>

- 14.3 The Supplier must ensure that any Supplier, Subcontractor, or Subprocessor system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified in the Order Form or otherwise in writing by the Buyer (where any such requirements have been provided).
- 14.4 If at any time the Supplier suspects or has reason to believe that the Government Data is corrupted, lost or sufficiently degraded, then the Supplier must immediately notify the Buyer and suggest remedial action.
- 14.5 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:
- 14.5.1 tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
 - 14.5.2 restore the Government Data itself or using a third party.
- 14.6 The Supplier must pay each Party's reasonable costs of complying with clause 14.5 unless the Buyer is at fault.
- 14.7 The Supplier:
- 14.7.1 must provide the Buyer with all Government Data in an agreed format (provided it is secure and readable) within 10 Working Days of a written request;
 - 14.7.2 must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
 - 14.7.3 must securely destroy all storage media that has held Government Data at the end of life of that media using Good Industry Practice, other than in relation to Government Data which is owned or licenced by the Supplier or in respect of which the Parties are Independent Controllers or Joint Controllers;
 - 14.7.4 securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it, other than in relation to Government Data which is owned or licenced by the Supplier or in respect of which the Parties are Independent Controllers or Joint Controllers; and
 - 14.7.5 indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation.
- 14.8 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 the Contract dictates the status of each party under the DPA 2018. A Party may act as:
- 14.8.1 "Controller" in respect of the other Party who is "Processor";
 - 14.8.2 "Processor" in respect of the other Party who is "Controller";
 - 14.8.3 "Joint Controller" with the other Party;
 - 14.8.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under the Contract and shall specify in Part A Authorised Processing Template of Annex 1 – Processing Personal Data which scenario they think shall apply in each situation.

14.9 Where one Party is Controller and the other Party its Processor

- 14.9.1 Where a Party is a Processor, the only processing that the Processor is authorised to do is listed in Part A Authorised Processing Template of Annex 1 – Processing Personal Data by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).
- 14.9.2 The Processor must notify the Controller immediately if it thinks the Controller's instructions breach the Data Protection Legislation.
- 14.9.3 The Processor must give all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment before starting any processing, which may include, at the discretion of the Controller:
 - 14.9.3.1 a systematic description of the expected processing and its purpose;
 - 14.9.3.2 the necessity and proportionality of the processing operations;
 - 14.9.3.3 the risks to the rights and freedoms of Data Subjects; and
 - 14.9.3.4 the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.
- 14.9.4 The Processor must, in relation to any Personal Data processed under this Contract:
 - 14.9.4.1 process that Personal Data only in accordance with Part A Authorised Processing Template of Annex 1 – Processing Personal Data unless the Processor is required to do otherwise by Law. If lawful to notify the Controller, the Processor must promptly notify the Controller if the Processor is otherwise required to process Personal Data by Law before processing it.
 - 14.9.4.2 put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Controller.
 - 14.9.4.3 Ensure that:
 - (a) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Part A Authorised Processing Template of Annex 1 – Processing Personal Data);
 - (b) it uses best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (i) are aware of and comply with the Processor's duties under this clause 14;
 - (ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

- (iii) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise allowed by the Contract; and
 - (iv) have undergone adequate training in the use, care, protection and handling of Personal Data.
- (c) the Processor must not transfer Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (d) the transfer is in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018) and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or
- (e) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or the transfer is in accordance with Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:
 - (i) where the transfer is subject to UK GDPR:
 - (A) the International Data Transfer Agreement (the “**IDTA**”), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018 as well as any additional measures determined by the Controller;
 - (B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (“**EU SCCs**”), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the “**Addendum**”) as published by the Information Commissioner's Office from time to time; and/or
 - (ii) where the transfer is subject to EU GDPR, the EU SCCs, as well as any additional measures determined by the Controller being implemented by the importing party;
- (f) the Data Subject has enforceable rights and effective legal remedies when transferred;
- (g) the Processor meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

- (h) the Processor complies with the Controller's reasonable prior instructions about the processing of the Personal Data.

- 14.9.5 The Processor must 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.
- 14.9.6 The Processor must notify the Controller immediately if it:
- 14.9.6.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
 - 14.9.6.2 receives a request to rectify, block or erase any Personal Data;
 - 14.9.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - 14.9.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
 - 14.9.6.5 receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; and
 - 14.9.6.6 becomes aware of a Data Loss Event.
- 14.9.7 Any requirement to notify under clause 14.9.6 includes the provision of further information to the Controller in stages as details become available.
- 14.9.8 The Processor must promptly provide the Controller with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.9.6. This includes giving the Controller:
- 14.9.8.1 full details and copies of the complaint, communication or request;
 - 14.9.8.2 reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
 - 14.9.8.3 any Personal Data it holds in relation to a Data Subject on request;
 - 14.9.8.4 assistance that it requests following any Data Loss Event; and
 - 14.9.8.5 assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office or any other regulatory authority.
- 14.9.9 The Processor must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Processor employs fewer than 250 staff, unless either the Controller determines that the processing:
- 14.9.9.1 is not occasional;

- 14.9.9.2 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
 - 14.9.9.3 is likely to result in a risk to the rights and freedoms of Data Subjects.
- 14.9.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 14.9.11 Before allowing any Subprocessor to process any Personal Data, the Processor must:
 - 14.9.11.1 notify the Controller in writing of the intended Subprocessor and processing;
 - 14.9.11.2 obtain the written consent of the Controller;
 - 14.9.11.3 enter into a written contract with the Subprocessor so that this clause 14 applies to the Subprocessor; and
 - 14.9.11.4 provide the Controller with any information about the Subprocessor that the Controller reasonably requires.
- 14.9.12 The Processor remains fully liable for all acts or omissions of any Subprocessor.
- 14.9.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other regulatory authority.

14.10 Joint Controllers of Personal Data

- 14.10.1 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 Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data.

14.11 Independent Controllers of Personal Data

- 14.11.1 In the event that the Parties are Independent Controllers in respect of Personal Data under the Contract, the terms set out in Part C Independent Controllers (*Optional*) of Annex 1 – Processing Personal Data shall apply to this Contract.

15 WHAT YOU MUST KEEP CONFIDENTIAL

- 15.1 Each Party must:
 - 15.1.1 keep all Confidential Information it receives confidential and secure;
 - 15.1.2 not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract; and
 - 15.1.3 immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.
- 15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:

- 15.2.1 where disclosure is required by applicable Law if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
 - 15.2.2 if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;
 - 15.2.3 if the information was given to it by a third party without obligation of confidentiality;
 - 15.2.4 if the information was in the public domain at the time of the disclosure;
 - 15.2.5 if the information was independently developed without access to the disclosing Party's Confidential Information;
 - 15.2.6 on a confidential basis, to its auditors or for the purposes of regulatory requirements;
 - 15.2.7 on a confidential basis, to its professional advisers on a need-to-know basis; and
 - 15.2.8 to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.
- 15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.
- 15.4 The Buyer may disclose Confidential Information in any of the following cases:
- 15.4.1 on a confidential basis to the employees, agents, consultants and contractors of the Buyer;
 - 15.4.2 on a confidential basis to any Crown Body, any successor body to a Crown Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;
 - 15.4.3 if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
 - 15.4.4 where requested by Parliament; and
 - 15.4.5 under clauses 5.7 and 16.
- 15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.
- 15.6 Transparency Information, and Information which is exempt from disclosure by clause 16 is not Confidential Information.
- 15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable endeavours to ensure that Supplier Staff do not either.

16 WHEN YOU CAN SHARE INFORMATION

- 16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.
- 16.2 In accordance with a reasonable timetable and in any event within 5 Working Days of a request from the Buyer, the Supplier must give the Buyer full co-operation and information needed so the Buyer can:
- 16.2.1 comply with any Request For Information
 - 16.2.2 if the Contract has a value over the relevant threshold in Part 2 of the Regulations, comply with any of its obligations in relation to publishing Transparency Information.
- 16.3 To the extent that it is allowed and practical to do so, the Buyer will use reasonable endeavours to notify the Supplier of a Request For Information and may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure is the Buyer's decision in its absolute discretion.

17 INSURANCE

- 17.1 The Supplier shall ensure it has adequate insurance cover for this Contract.

18 INVALID PARTS OF THE CONTRACT

- 18.1 If any provision or part-provision of this Contract is or becomes invalid, illegal or unenforceable for any reason, such provision or part-provision shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Contract. The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements, or agreements whether written or oral. No other provisions apply.

19 OTHER PEOPLE'S RIGHTS IN THE CONTRACT

- 19.1 No third parties may use the Contracts (Rights of Third Parties) Act ("**CRTPA**") to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20 CIRCUMSTANCES BEYOND YOUR CONTROL

- 20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Contract while the inability to perform continues, if it both:
- 20.1.1 provides written notice to the other Party; and
 - 20.1.2 uses all reasonable measures practical to reduce the impact of the Force Majeure Event.
- 20.2 Any failure or delay by the Supplier to perform its obligations under the Contract that is due to a failure or delay by an agent, Subcontractor and/or Supplier Staff will only be considered a Force Majeure Event if that third party is itself prevented from complying with an obligation to the Supplier due to a Force Majeure Event.

20.3 Either Party can partially or fully terminate the Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously and the consequences of termination in Clauses 11.5.1.2 to 11.5.1.7 shall apply.

20.4 Where a Party terminates under clause 20.3:

20.4.1 each Party must cover its own losses; and

20.4.2 clauses 11.5.1.2 to 11.5.1.7 apply.

21 RELATIONSHIPS CREATED BY THE CONTRACT

21.1 The Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22 GIVING UP CONTRACT RIGHTS

22.1 A partial or full waiver or relaxation of the terms of the Contract is only valid if it is stated to be a waiver in writing to the other Party.

23 TRANSFERRING RESPONSIBILITIES

23.1 The Supplier cannot assign, novate or in any other way dispose of the Contract or any part of it without the Buyer's written consent.

23.2 The Buyer can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Buyer.

23.3 When the Buyer uses its rights under clause 23.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.

23.4 The Supplier can terminate the Contract novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

24 SUPPLY CHAIN

24.1 The Supplier cannot sub-contract the Contract or any part of it without the Buyer's prior written consent. The Supplier shall provide the Buyer with the name of any Subcontractor the Supplier proposes to engage for the purposes of the Contract. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. If the Buyer does not communicate a decision to the Supplier within 10 Working Days of the request for consent then its consent will be deemed to have been given. The Buyer may reasonably withhold its consent to the appointment of a Subcontractor if it considers that:

24.1.1 the appointment of a proposed Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

24.1.2 the proposed Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

- 24.1.3 the proposed Subcontractor employs unfit persons.
- 24.2 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of all such Subcontractors at all levels of the supply chain including:
 - 24.2.1 their name;
 - 24.2.2 the scope of their appointment; and
 - 24.2.3 the duration of their appointment.
- 24.3 The Supplier must exercise due skill and care when it selects and appoints Subcontractors.
- 24.4 For Sub-Contracts in the Supplier's supply chain entered into wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract:
 - 24.4.1 where such Sub-Contracts are entered into after the Start Date, the Supplier will ensure that they all contain provisions that; or
 - 24.4.2 where such Sub-Contracts are entered into before the Start Date, the Supplier will take all reasonable endeavours to ensure that they all contain provisions that:
 - 24.4.2.1 allow the Supplier to terminate the Sub-Contract if the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law;
 - 24.4.2.2 require the Supplier to pay all Subcontractors in full, within 30 days of receiving a valid, undisputed invoice; and
 - 24.4.2.3 allow the Buyer to publish the details of the late payment or non-payment if this 30-day limit is exceeded.
- 24.5 At the Buyer's request, the Supplier must terminate any Sub-Contracts in any of the following events:
 - 24.5.1 there is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 of a Subcontractor which isn't pre-approved by the Buyer in writing;
 - 24.5.2 the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 11.4;
 - 24.5.3 a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Buyer;
 - 24.5.4 the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law; and/or
 - 24.5.5 the Buyer has found grounds to exclude the Subcontractor in accordance with Regulation 57 of the Regulations.
- 24.6 The Supplier is responsible for all acts and omissions of its Subcontractors and those employed or engaged by them as if they were its own.

25 CHANGING THE CONTRACT

- 25.1 Either Party can request a variation to the Contract which is only effective if agreed in writing and signed by both Parties. The Buyer is not required to accept a variation request made by the Supplier.

26 HOW TO COMMUNICATE ABOUT THE CONTRACT

- 26.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9am on the first Working Day after sending unless an error message is received.
- 26.2 Notices to the Buyer or Supplier must be sent to their address or email address in the Order Form.
- 26.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

27 DEALING WITH CLAIMS

- 27.1 If a Beneficiary becomes aware of any Claim, then it must notify the Indemnifier as soon as reasonably practical.
- 27.2 at the Indemnifier's cost the Beneficiary must:
- 27.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim;
 - 27.2.2 give the Indemnifier reasonable assistance with the Claim if requested; and
 - 27.2.3 not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.
- 27.3 The Beneficiary must:
- 27.3.1 consider and defend the Claim diligently and in a way that does not damage the Beneficiary's reputation; and
 - 27.3.2 not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

28 PREVENTING FRAUD, BRIBERY AND CORRUPTION

- 28.1 The Supplier shall not:
- 28.1.1 commit any criminal offence referred to in 57(1) and 57(2) of the Regulations; or
 - 28.1.2 offer, give, or agree to give anything, to any person (whether working for or engaged by the Buyer or any other public body) an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Contract or any other public function or for showing or refraining from showing favour or disfavour to any person in relation to the Contract or any other public function.

- 28.2 The Supplier shall take all reasonable endeavours (including creating, maintaining and enforcing adequate policies, procedures and records), in accordance with Good Industry Practice, to prevent any matters referred to in clause 28.1 and any fraud by the Supplier Staff and the Supplier (including its shareholders, members and directors) in connection with the Contract and shall notify the Buyer immediately if it has reason to suspect that any such matters have occurred or is occurring or is likely to occur.
- 28.3 If the Supplier notifies the Buyer as required by clause 28.2, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.
- 28.4 If the Supplier or the Supplier Staff engages in conduct prohibited by clause 28.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Buyer) the Buyer may:
- 28.4.1 require the Supplier to remove any Supplier Staff from providing the Deliverables if their acts or omissions have caused the default; and
 - 28.4.2 immediately terminate the Contract and the consequences of termination in Clause 11.5.1 shall apply.

29 EQUALITY, DIVERSITY AND HUMAN RIGHTS

- 29.1 The Supplier must follow all applicable employment and equality Law when they perform their obligations under the Contract, including:
- 29.1.1 protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
 - 29.1.2 any other requirements and instructions which the Buyer reasonably imposes related to equality Law.
- 29.2 The Supplier must use all reasonable endeavours, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

30 HEALTH AND SAFETY

- 30.1 The Supplier must perform its obligations meeting the requirements of:
- 30.1.1 all applicable Law regarding health and safety; and
 - 30.1.2 the Buyer's current health and safety policy while at the Buyer's premises, as provided to the Supplier.
- 30.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer premises that relate to the performance of the Contract.

31 ENVIRONMENT AND SUSTAINABILITY

31.1 In performing its obligations under the Contract, the Supplier shall, to the reasonable satisfaction of the Buyer:

- 31.1.1 meet, in all material respects, the requirements of all applicable Laws regarding the environment; and
- 31.1.2 comply with its obligations under the Buyer's current environmental policy, which the Buyer must provide, and make Supplier Staff aware of such policy.

32 TAX

32.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Contract where the Supplier has not paid a minor tax or social security contribution.

32.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Contract, the Supplier must both:

- 32.2.1 comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
- 32.2.2 indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

32.3 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains requirements that:

- 32.3.1 the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 32.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
- 32.3.2 the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
- 32.3.3 the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with clause 32.2 or confirms that the Worker is not complying with those requirements; and
- 32.3.4 the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

33 CONFLICT OF INTEREST

- 33.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual, potential or perceived Conflict of Interest.
- 33.2 The Supplier must promptly notify and provide details to the Buyer if an actual, potential or perceived Conflict of Interest happens or is expected to happen.
- 33.3 The Buyer will consider whether there are any appropriate measures that can be put in place to remedy an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Buyer, such measures do not or will not resolve an actual or potential conflict of interest, the Buyer may terminate the Contract immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest and Clauses 11.5.1.2 to 11.5.1.7 shall apply.

34 REPORTING A BREACH OF THE CONTRACT

- 34.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of Law, clause 13.1, or clauses 27 to 33.
- 34.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 34.1 to the Buyer or a Prescribed Person.

35 FURTHER ASSURANCES

- 35.1 Each Party will, at the request and cost of the other Party, do all things which may be reasonably necessary to give effect to the meaning of this Contract.

36 RESOLVING DISPUTES

- 36.1 If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute by commercial negotiation.
- 36.2 If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (“CEDR”) Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 36.3 to 36.5.
- 36.3 Unless the Buyer refers the dispute to arbitration using clause 36.4, the Parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction. :
- 36.4 The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

36.5 The Buyer has the right to refer a dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 36.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 36.4.

36.6 The Supplier cannot suspend the performance of the Contract during any dispute.

37 WHICH LAW APPLIES

37.1 This Contract and any issues or disputes arising out of, or connected to it, are governed by English law.

III. **Annex 1 – Processing Personal Data**

Part A Authorised Processing Template

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

■ The contact details of the Controller's Data Protection Officer are: ■ ■

The contact details of the Processor's Data Protection Officer are: ■

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

Any such further instructions shall be incorporated into this Annex.

Description of authorised processing	Details
Identity of Controller and Processor / Independent Controllers / Joint Controllers for each category of Personal Data	None for personal data
Subject matter of the processing	Redacted layout plans PDF drawings of the sites identified for survey.
Duration of the processing	10th February to 31st March 2025
Nature and purposes of the processing	Evaluation of building information for purposes of specialist site surveys (visual impairment)
Type of Personal Data being processed	None
Categories of Data Subject	Building Information, plans
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	Destruction post receipt of finalised reports and close out of follow up calls.
Locations at which the Supplier and/or its Subcontractors process Personal Data under this Contract	n/a

and International transfers and legal gateway	
Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect Personal Data processed under this Contract against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event	n/a

Part B Joint Controller Agreement (*Optional*)

Not Used

38 LIABILITIES FOR DATA PROTECTION BREACH

- 38.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Data Loss Event ("**Financial Penalties**") then the following shall occur:
- 38.1.1 if in the view of the Information Commissioner, the Buyer is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Data Loss Event. The Supplier shall provide to the Buyer 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 Data Loss Event;
 - 38.1.2 if in the view of the Information Commissioner, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Data Loss Event; or
 - 38.1.3 if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Data Loss Event and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Data Loss Event 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 36 of the Conditions (Resolving disputes).

- 38.2 If either the Buyer 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 Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 38.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "**Claim Losses**"):
- 38.3.1 if the Buyer is responsible for the relevant Data Loss Event, then the Buyer shall be responsible for the Claim Losses;
 - 38.3.2 if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and
 - 38.3.3 if responsibility for the relevant Data Loss Event is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.
- 38.4 Nothing in either Paragraph 38.2 or Paragraph 38.3 of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data shall preclude the Buyer 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 Data Loss Event, having regard to all the circumstances of the Data Loss Event and the legal and financial obligations of the Buyer.

39 TERMINATION

- 39.1 If the Supplier is in Material Breach under any of its obligations under this of this Part B Joint Controller Agreement (*Optional*) of Annex 1 – Processing Personal Data;, the Buyer shall be entitled to terminate the Contract by issuing a termination notice to the Supplier in accordance with clause 11 of the Conditions (Ending the contract).

40 SUB-PROCESSING

- 40.1 In respect of any processing of Personal Data performed by a third party on behalf of a Party, that Party shall:
- 40.1.1 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
 - 40.1.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

41 DATA RETENTION

- 41.1 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 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.

Part C Independent Controllers (*Optional*)

Not Used

IV.

Annex 2 – Specification

1. The Statement of Requirements and Scope

ANNEX 1

DWP Visual Impaired Access Pilot

1. Background to the Client

The Department for Work and Pensions (the **Client**) is responsible for welfare, pensions and child maintenance policy. As the UK's biggest public service department, it administers the State Pension and a range of working age, disability and ill health benefits to around 20 million claimants and customers.

The Client delivers these services across England, Wales and Scotland across a diverse estate of c.715 buildings. This number is made up primarily of Job Centre Plus offices, which the Client refers to as its 'front-of-House' estate, but also includes Health Assessment Centres and back offices. The back-office sites or 'back-of-House' estate consists of corporate centres, large processing centres and service centres very similar to call centre environments, which are not open to the public. The Client's estate is geographically dispersed due to the high street nature of the Job Centre Plus and Health Assessment Centre portfolio - requiring local presence to serve customers.

2. Background to the Client's Requirements

The DWP Design Standards Team wish to review and update guidance to inform inclusive design for our buildings and adaptations under reasonable adjustments (RAST).

This approach was selected to support the DWP Design Team in the requirement of a service to obtain impartial and independent advice from a national and respected authority in the UK. By commissioning "sample" surveys across a range of sites DWP hope to gain valuable independent insight to inform DWP's approach to the wider estate and RAST.

A one off pilot of four DWP sites is proposed to complement existing options, by exploring independent and impartial advice from the Royal National institute(s) of blind people (RNIB), the nation's leading sight loss charity in the UK.

This pilot would demonstrate positive action regarding inclusion and is intended to discover additional benefits over what existing/other supply chain options could provide, develop DWP's greater understanding as the DWP intelligent client, innovate and update DWP design standards guidance, and share outputs with the Accessibility Services supplier who will be appointed after April 2025, and project delivery e.g. RAST.

3. The Client's Requirements

This requirement is for the Supplier to:

1. Inclusive Design Site Appraisal:

- Site, Streets, and Surroundings: Assess external design elements such as parking, entrances, building access, and signage.
- Indoor Space Design: Evaluate features like lighting, surface contrast, furniture, wayfinding, navigation, and signage.
- Building Facilities: Review facilities including toilets and kitchenettes.

2. Comprehensive Report:

- Identify barriers or challenges that could hinder the inclusion of individuals with disabilities and accessibility needs.
- Provide recommended solutions categorised into priorities:
 - Priority 1: Health and safety issues requiring urgent attention.
 - Priority 2: Significant barriers for visually disabled people.
 - Priority 3: Expected requirements as per statutory regulations.
 - Priority 4: Issues to be addressed during routine maintenance, refurbishment, or upgrades.

3. Post-Completion:

- Conduct a one-hour online dissemination session with a Q&A about uplifting physical environments.
- Issue a commendation after implementing the recommendations

This 'Service' is required from contract award until 31 March 2025.

The proposed sites for surveys are:

- **Hub (Yorkshire: Sheffield Kings Court)**
- **Service Centre (Central: Pedmore House)**
- **JCP – Medium (Southern: Worthing Crown House)**
- **JCP – Small (Wales: Pwllheli Lower Cardiff Road)**
- **Plus, Quarry House on a call off basis if time allows.** (However, the call off scope is not yet determined for this site as DWP wish to develop and agree the scope under the supplier's day rate. DWP will not use this facility if they run out of time, and the scope will be tailored to specific requirements agreed within the available time.

b) Client Data

Data may be shared with and accessed by the Consultant as part of this contract.

All data will have Government Security Classification of OFFICIAL and may also be marked as OFFICIAL-SENSITIVE. The Consultant shall advise the Client regarding whether particular data would be needed.

c) Site Visits

Consultant Personnel must be fully attuned to the Client's business environment and the sensitive nature of the Client's operations. When conducting site visits, Consultant Personnel must ensure photographs taken do not record identifiable images of other persons or elements of the Client's operations beyond the scope of this Statement of Requirements and Scope.

d) Consultant Personnel Requirements

The Client requires that all Consultant staff employed, whether permanent or temporary, on the provision of the services are subject to the requirements of the HM Government Baseline Personnel Security Standard (BPSS).

There is no requirement to apply to the Client or any other third party for BPSS clearance. BPSS clearance is obtained if the following steps have been completed as part of your organisation's pre-employment checks:

- Verification of identity
- Verification of Nationality and Immigration Status (including an entitlement to undertake the work in question)
- Verification of Employment history (past 3 years)
- Verification of Criminal record (unspent convictions only). This will require a basic disclosure certificate (at cost via Disclosure and Barring Service, Disclosure Scotland and Access Northern Ireland).

Copies of the current HM Government Baseline Personnel Security Standard, providing further information regarding how each of these steps should be verified, can be found via the following link [Government Baseline Personnel Security Standard](#). The Consultant is expected to arrange the BPSS checks at no additional charge.

All personnel must comply with the Client's Security Policy (Annex 2). The Consultant will only be expected to comply with those Security Policies and Standards that are applicable to their delivery model and technologies used.

The Consultant must be able to immediately (on contract award) resource this requirement with Consultant personnel meeting the requirements of this section d).

Annex 1 - Security Policy**1. GENERAL**

The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with the Client's security requirements as set out in the Contract which include the requirements set out in this Annex 1 (the "**Security Policy**"). The Security Policy includes, but is not limited to, requirements regarding the confidentiality, integrity and availability of Client Assets, the Client's Systems Environment and the Consultant's Systems Environment.

Terms used in this Annex 3 which are not defined below shall have the meanings given to them in the Contract Data and/or clause Z1 (Interpretation and the law) of the Contract.

"Availability Test"	shall mean the activities performed by the Consultant to confirm the availability of any or all components of any relevant ICT system as specified by the Client.
"Breach of Security"	means the occurrence of: (I) any unauthorised access to or use of Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof); (II) the loss and/or unauthorised disclosure of any Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof); (III) any unauthorised event resulting in loss of availability of any Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof);

	(IV) any unauthorised changes or modification to any Client Data, the Client's Systems Environment (or any part thereof) or the Consultant's Systems Environment (or any part thereof).
"CHECK"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"Client Assets"	mean any Client Devices and Client Data.
"Client Data"	<p>means the data, guidance, specifications, instructions, toolkits, plans, databases, patents, patterns, models, design, 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, and which are:-</p> <p>(i) supplied to the Consultant by or on behalf of the Client; or</p> <p>(ii) which the Consultant is required to generate, process, store or transmit pursuant to this contract.</p>
"Client's Systems Environment"	means all of the Client's ICT systems which are or may be used for the provision of the <i>services</i> .
"Cloud"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.

“Consultant’s Systems Environment”	means any ICT systems provided by the Consultant (and any Sub-consultant) which are or may be used for the provision of the <i>services</i> .
“Cyber Essentials”	shall mean the Government-backed, industry-supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
“Cyber Security Information Sharing Partnership” or “CiSP”	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
“Client’s Systems Environment”	means all of the Client’s ICT systems which are or may be used for the provision of the <i>services</i> .
“Good Security Practice”	<p>shall mean:</p> <ul style="list-style-type: none"> a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology); b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided

	<p>to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and</p> <p>c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.</p>
"Information Security"	<p>shall mean:</p> <p>a) the protection and preservation of:</p> <p>i) the confidentiality, integrity and availability of any Client Assets, the Client's Systems Environment (or any part thereof) and the Consultant's Systems Environment (or any part thereof);</p> <p>ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and</p> <p>b) compliance with all Law applicable to the processing, transmission, storage and disposal of Client Assets.</p>
"Information Security Manager"	<p>shall mean the person appointed by the Consultant with the appropriate experience, authority and expertise to ensure that the Consultant complies with the Security Policy.</p>
"Information Security Management System ("ISMS")"	<p>shall mean the set of policies, processes and systems designed, implemented and maintained by the Consultant to manage Information Security Risk as specified by ISO/IEC 27001.</p>
"Information Security Questionnaire"	<p>shall mean the Client's set of questions used to audit and on an ongoing basis assure the Consultant's compliance with the Security</p>

	Policy. The Information Security Questionnaire is the Security Management Plan.
“Information Security Risk”	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
“ISO/IEC 27001, ISO/IEC 27002 and ISO 22301	<p>shall mean</p> <p>a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301</p> <p>in each case as most recently published by the International Organization for Standardization or its successor entity (the “ISO”) or the relevant successor or replacement information security standard which is formally recommended by the ISO.</p>
“NCSC”	shall mean the National Cyber Security Centre or its successor entity (where applicable).
“Penetration Test”	shall mean a simulated attack on any Client Assets, the Client’s Systems Environment (or any part thereof) or the Consultant’s Systems Environment (or any part thereof).
“PCI DSS”	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the “PCI”).
“Risk Profile”	shall mean a description of any set of risk. The set of risks can contain those that relate

	to a whole organisation, part of an organisation or as otherwise applicable.
“Security Test”	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
“Security Policies”	mean the Client’s Security Policies published by the Client from time to time and shall include any successor, replacement or additional Security Policies. The Security Policies are set out in Annex A.
“Security Policies and Standards”	mean the Security Policies and the Security Standards
“Security Standards”	mean the Client’s Security Standards published by the Client from time to time and shall include any successor, replacement or additional Security Standards. The Security Standards are set out in Annex B.
“Tigerscheme”	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
“Vulnerability Scan”	shall mean an ongoing activity to identify any potential vulnerability in any Client Assets, the Client’s Systems Environment (or any part thereof) or the Consultant’s Systems Environment (or any part thereof).

- 1.1 Reference to any notice to be provided by the Consultant to the Client shall be construed as a notice to be provided by the Consultant to the Client.

2. PRINCIPLES OF SECURITY

- 2.1 The Consultant shall at all times comply with the Security Policy and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

- 3.1 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with ISO/IEC 27001 in relation to the *services* during the Contract.
- 3.2 The Consultant shall appoint an Information Security Manager and shall notify the Client of the identity of the Information Security Manager on the *starting date* and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.
- 3.3 The Consultant shall ensure that it operates and maintains the Information Security Management System during the *service period* and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:
- a) a scope statement (which covers all of the Services provided under this Contract);
 - b) a risk assessment (which shall include any risks specific to the Services);
 - c) a statement of applicability;
 - d) a risk treatment plan; and
 - e) an incident management plan
- in each case as specified by ISO/IEC 27001.

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

- 3.3A If the Consultant reasonably considers that it is not reasonably commercially possible for it to comply with paragraphs 3.1 and 3.3 of this Schedule by the start of the *service period*, the Consultant shall:
- a) give written notice to the Client to inform it of the same and complete, in cooperation with the Client, the Information Security Questionnaire within 5 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract in accordance with paragraph 6.1 of this Schedule;
 - b) provide to the Client, for its consideration, within 10 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract:
 - i. a proposed action plan (including a timetable) indicating how the Consultant will become compliant with paragraphs 3.1 and 3.3 of this Schedule and the dates by which they can reasonably become compliant (assuming the Consultant uses all reasonable endeavours to do so) ("**Proposed ISO27001 Action Plan**"); and
 - ii. its proposed Information Security Management System that mitigates the failure to comply with paragraphs 3.1 and 3.3 of this Schedule as far as reasonably commercially possible and which is otherwise compliant with the requirements of this Schedule ("**Proposed ISMS**"),

and the Consultant shall make such amendments to the Proposed ISO27001 Action Plan and the Proposed ISMS that the Client shall consider necessary in the interests of complying with this Schedule and managing Information Security Risk. Upon the Client being satisfied with

the Proposed ISO27001 Action Plan and Proposed ISMS (following implementation of such amendments it considers necessary) it shall notify the Consultant, upon which they shall become the “**ISO27001 Action Plan**” and “**Interim ISMS**” respectively;

- c) use all reasonable endeavours to become compliant with paragraphs 3.1 and 3.3 of this Schedule as soon as possible and in any event shall become compliant by no later than the dates set out in the ISO27001 Action Plan; and
- d) operate and maintain the Proposed ISMS until such time as the Interim ISMS is approved, upon which it will operate and maintain the Interim ISMS, as modified from time to time pursuant to the implementation of the ISO27001 Action Plan.

Any breach of this paragraph 3.3A constitutes a substantial failure to comply with the Consultant's obligations under the Contract.

- 3.4 The Consultant shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Client.
- 3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Client may, in its absolute discretion, notify the Consultant that it is not in compliance with the Security Policy and provide details of such non-compliance. The Consultant shall, at its own expense, undertake those actions required in order to comply with the Security Policy within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Security Policy within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a substantial failure by the Consultant to comply with his obligations.

4. CYBER ESSENTIALS SCHEME

- 4.1 The Consultant shall, and shall procure that any Sub-Consultant (as applicable) shall, obtain and maintain certification to Cyber Essentials (the “Cyber Essentials Certificate”) in relation to the Services during the *service period*. The Cyber Essentials Certificate shall be provided by the Consultant to the Client annually on the dates as agreed by the Parties.
- 4.2 The Consultant shall notify the Client of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Consultant shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the *service period* after the first date on which the Consultant was required to provide a Cyber Essentials Certificate in accordance with paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy) shall constitute a substantial failure by the Consultant to comply with his obligations.
- 4.3 If the Consultant reasonably considers that it is not reasonably commercially possible for it to obtain certification to Cyber Essentials by the start of the *service period*, the Consultant shall:

- a) give written notice to the Client to inform it of the same and complete, in cooperation with the Client, the Information Security Questionnaire within 5 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract in accordance with paragraph 6.1 of this Schedule;
- b) provide to the Client, for its consideration, within 10 working days of being notified by the Client that the Consultant is the successful Framework Supplier (as defined in the Framework Agreement) in respect of this Contract, a proposed action plan (including a timetable) indicating how certification to Cyber Essentials will be obtained and the date by which it will be obtained (assuming the Consultant uses all reasonable endeavours to do so) ("**Proposed CEP Action Plan**") and the Consultant shall make such amendments to the Proposed CEP Action Plan that the Client shall consider necessary in the interests of complying with this Schedule and managing Information Security Risk. Upon the Client being satisfied with the Proposed CEP Action Plan (following implementation of such amendments it considers necessary) it shall notify the Consultant, upon which it shall become the "**CEP Action Plan**"; and
- c) use all reasonable endeavours to obtain certification to Cyber Essentials soon as possible and in any event shall become compliant by no later than the dates set out in the CEP Action Plan.

Any breach of this paragraph 4.3 constitutes a substantial failure to comply with the Consultant's obligations under the Contract.

5. RISK MANAGEMENT

- 5.1 The Consultant shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the *service period* which includes standards and processes for the assessment of any potential risks in relation to the *services* and processes to ensure that the Security Policy is met (the **Risk Assessment**). The Consultant shall provide the Risk Management Policy to the Client upon request within 10 Working Days of such request. The Client may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Security Policy. The Consultant shall, at its own expense, undertake those actions required in order to implement the changes required by the Client within one calendar month of such request or on a date as agreed by the Parties.
- 5.2 The Consultant shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Consultant's Systems Environment or in the threat landscape or (iii) at the request of the Client. The Consultant shall provide the report of the Risk Assessment to the Client, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Consultant shall notify the Client within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.
- 5.3 If the Client decides, at its absolute discretion, that any Risk Assessment does not meet the Security Policy, the Consultant shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.
- 5.4 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, co-operate with the Client in relation to the Client's own risk management processes regarding the *services*.

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

6. SECURITY AUDIT AND ASSURANCE

- 6.1 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, complete the information security questionnaire in the format stipulated by the Client (the “**Information Security Questionnaire**”) at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.
- 6.2 The Consultant shall conduct Security Tests to assess the Information Security of the Consultant’s Systems Environment and, if requested, the Client’s Systems Environment. In relation to such Security Tests, the Consultant shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Consultant’s Systems Environment or in the Client’s System Environment or (iii) at the request of the Client which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Client. The Consultant shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Consultant shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Client in its absolute discretion.
- 6.3 The Client shall be entitled to send an agent appointed by it, or such other person it shall reasonably require to witness the conduct of any Security Test. The Consultant shall provide to the Client notice of any Security Test at least one month prior to the relevant Security Test.
- 6.4 Where the Consultant provides code development services to the Client, the Consultant shall comply with the Security Policy in respect of code development within the Consultant’s Systems Environment and the Client’s Systems Environment.
- 6.5 Where the Consultant provides software development services, the Consultant shall comply with the code development practices specified in the Statement of Requirements and Scope or in the Security Policy.
- 6.6 The Client, or an agent appointed by it, may undertake Security Tests in respect of the Consultant’s Systems Environment after providing advance notice to the Consultant. If any Security Test identifies any non-compliance with the Security Policy, the Consultant shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner

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

- 6.7 The Client shall schedule regular security governance review meetings which the Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, attend.

7. PCI DSS COMPLIANCE AND CERTIFICATION

- 7.1 Where the Consultant obtains, stores, processes or transmits payment card data, the Consultant shall comply with the PCI DSS.
- 7.2 The Consultant shall obtain and maintain up-to-date attestation of compliance certificates (“**AoC**”) provided by a qualified security assessor accredited by the PCI and up-to-date self-assessment questionnaires (“**SAQ**”) completed by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the “PCI Reports”), during the *service period*. The Consultant shall provide the respective PCI Reports to the Client upon request within 10 Working Days of such request.
- 7.3 The Consultant shall notify the Client of any failure to obtain a PCI Report or a revocation of a PCI Report within 2 Working Days of confirmation of such failure or revocation. The Consultant shall, at its own expense, undertake those actions required in order to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

8. SECURITY POLICIES AND STANDARDS

- 8.1 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.
- 8.2 Notwithstanding the foregoing, the Security Policy applicable to the services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. The Client may issue instructions to the Consultant to comply with any amended Security Policy as required by the Client, provided that where such amended Security Policy increases the burden on the Consultant pursuant to this contract, the novation shall be a compensation event. Accordingly a new clause 60.1(14) shall be added that reads “An amendment to a Security Policy pursuant to paragraph 8.2 of Contract Schedule 8 occurs which increases the burden on the Consultant pursuant to this Contract”.
- 8.3 The Consultant shall, and shall procure that any Sub-consultant (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

9. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

- 9.1 The Consultant may become a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the *service period*. The Consultant may participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.
- 9.2 Where the Consultant becomes a member of the Cyber Security Information Sharing Partnership, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Consultant's Risk Management Policy.

ANNEX A – CLIENT SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

<https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards> unless specified otherwise:

- a) Acceptable Use Policy
- b) Information Security Policy
- c) Physical Security Policy
- d) Information Management Policy
- e) Email Policy
- f) Technical Vulnerability Management Policy
- g) Remote Working Policy
- h) Social Media Policy
- i) Forensic Readiness Policy
- j) SMS Text Policy
- k) Privileged Users Security Policy
- l) User Access Control Policy
- m) Security Classification Policy
- n) Cryptographic Key Management Policy
- o) HMG Personnel Security Controls – May 2018
(published on <https://www.gov.uk/government/publications/hmg-personnel-security-controls>)
- p) NCSC Secure Sanitisation of Storage Media
(published on <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:

<https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards>:

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

Annex 2 - The Client's Expenses Policy

Circumstances where the *Employer* will not reimburse expenses incurred

1.1 The *Employer* will not reimburse routine costs incurred for travel to, or accommodation at, DWP project sites.

1.2 The *Employer* will not pay or be responsible for the payment of any fines or penalty charges in respect of private vehicles etc. during the undertaking of duties for the *Employer*.

2. Circumstances where the *Employer* will reimburse expenses incurred

2.1 The *Employer* will re-imburse necessary and reasonable business travel and accommodation costs incurred during the undertaking of duties for the *Employer* subject to the following:

2.1.1 All such expenses being agreed with the *Employer* in advance.

2.1.2 The rules for claiming expenses must be in accordance with this Contract Schedule 8 at the time the expense is incurred.

2.1.3 The Task requires a significantly higher volume of travel or accommodation than may usually be expected in the usual course of business.

2.1.4 All such expenses must have been incurred in performing the *services* away from their main base location and are minus the cost of travel to the usual place of work.

2.1.5 Appropriate documentary evidence, such as receipts and tickets, of such expenses being incurred is provided to the *Employer*.

2.1.6 The expenses must be submitted at the same time as the relevant timesheet.

3. General statements on Business Travel and Accommodation

3.1 Before committing to any travel arrangements the *Consultant* must discuss travelling needs with the *Employer* and assess whether the following could be used:

3.1.1 Video conferencing

3.1.2 Telephone conferencing

3.1.3 Web conferencing

3.1.4 Audio conferencing

3.1.5 The business needs to travel

3.1.6 The most economical and suitable means of travel, considering value for money and sustainability factors.

3.2 Business journeys must only be made when site attendance or face-to-face meetings is essential. Authorisation to travel must be received from the *Employer* before committing to make travel arrangements.

3.3 The most cost effective/value for money option should be obtained and the *Consultant* can use their own organisations' booking agent(s) or low-cost alternatives. Advantage should be taken of any offers for reduced travel (including advanced-purchase tickets/advanced-booking for rooms) or room rates. Alternatively, any claims for the cost of travel and accommodation must be evidenced with supporting documentation and receipts.

3.4 No organisational or personal benefit must be obtained arising from the promotions, offers, or reward schemes that ensue from official travel or accommodation paid for by the *Employer*, whether in advance or by refund. Where such promotions or offers are available, the *Consultant* should agree with the *Employer*, whenever possible, how to use any such benefits to offset against other expenses payable by the *Employer*.

3.5 The *Employer* reserves the right to reject claims for unreasonable expenses, or expenses which could have been avoided if a journey had been better planned.

4. Rates and Expenses Type

4.1 The types of expenses and the rates payable are given at Annex 1. The rates payable are subject to change.

4.2 Claims for mobile phone calls and internet use - costs for mobile telephone calls and Internet use cannot be claimed.

4.3 Public transport including rail travel - on public transport standard class travel must be used. First class travel is strictly prohibited irrespective of the duties undertaken.

4.4 The use of rail, 'Oyster' and other discount cards or schemes is encouraged if evidence is shown that these will save the *Employer* more than their cost.

4.5 Taxis - taxi fares may be reimbursed for business travel where their use is reasonable in the circumstances. Actual fares only can be claimed in the following circumstances:

4.5.1 Where there is no other suitable method of public transport

4.5.2 In exceptional and infrequent circumstances where the saving of official time is important

4.5.3 When heavy luggage must be handled

4.5.4 When shared by colleagues and the fare overall is cheaper than public transport

4.6 Air travel: claims for domestic air travel are not permitted unless the flight is over 300 miles. This limit is for one-way flights within the British mainland. For travel between the destinations shown below air travel is not permitted, journeys must be taken by rail:

4.6.1 Newcastle and London

4.6.2 Birmingham and Newcastle

4.6.3 Manchester and London

4.7 Economy-class air travel must always be booked when travelling on domestic flights within the UK. No business-class or first-class tickets must be booked on domestic flights regardless of the length/duration of journey.

4.8 Private motor vehicles and private vehicle use: the *Employer* aims to reduce mileage travelled in private motor vehicles undertaken by consultants. When considering the use of a vehicle on official business, the *Consultant* must only use their own vehicle for business journeys when there is no other practicable mode of transport including public transport. Permission must be gained from the *Employer* for each business journey carried out in a private vehicle.

4.9 Before undertaking such journeys the *Employer* must check that the *Consultant* holds a full current driving license. The private vehicle must be roadworthy and, where required, have a valid 'MOT' test certificate. The *Contractor's* personnel must ensure their motor vehicle insurance policy includes an 'employer indemnity' clause in addition to a business-use clause. It is the policyholder's responsibility to check with their insurance company that they have both types of cover. There are mileage restrictions of a maximum of 1,000 miles per financial year and 100 miles per day once authorisation has been obtained. Where the *Consultant* genuinely needs to travel more than 1,000 miles per year or 100 miles per day in their own vehicle, they must have written permission from the *Employer* in the form of business case authorised at least UG7 Grade. For daily journeys over 100 miles, an exemption is required only if it is likely to be a regular occurrence. One -off situations can be approved locally with no form required.

4.10 Reasons for granting permission must be clearly documented in a business case, whose format is identified at Annex 2, and retained for audit purposes.

4.11 Car park fees can be claimed on production of the appropriate documentary evidence. Receipts should be retained and provided to the *Employer*. However, the *Employer* will not provide remuneration for travel on toll-roads.

5. Overnight Accommodation

5.1 Hotel: where it is necessary for the *Consultant* to stay away from their main base location(s) to provide the services, then:

5.1.1 Expenses will only be reimbursed where it is not possible for the *Consultant* to stay at their home.

5.1.2 The following two principles must apply to any accommodation booking:

5.1.2.1 It must be as close to the site as possible and within a 5-mile radius; and

5.1.2.2 It must be the most economical option, having considered the whole trip cost, such as public transport costs, taxi fares and travelling time.

5.2 Regional maximum limits for claims for overnight hotel accommodation are included at Annex 1.

5.3 Lodging rate: where the *Consultant* elects to stay with friends or relatives rather than in a hotel or other commercial establishment, then the hotel rates do not apply. The lodging rate is payable at a flat rate to cover accommodation.

Annex 1

Expenses rates:

- *Expenses* are listed in the Travel & Accommodation Expenses tab within Attachment 4 – Commercial Envelope.

Expenses shall not be adjusted using Secondary Option X1 (Adjustment for inflation). The *expenses* are adjusted when the *Employer* makes an adjustment to the rates, and is at the sole discretion of the *Employer*.

Annex 2

Business case for approval to exceed the *Employer's* mileage restrictions of 100 miles per day or 1,000 miles per year:

Business unit:	
Name of proposer:	
Grade of proposer:	
Home Office:	
Name of staff the exemption covers:	
Short description of journeys undertaken including daily mileage:	
Are there any reasons, through health or disability, that an exemption should be granted:	
If yes do not fill in any further.	
Reasons why tele-conference or video conference are unsuitable:	
Reasons why public transport is unsuitable:	
Authorising person:	
Grade of authorising person:	
Date:	

When exemption is granted, please retain a copy of this form for audit purposes.

V. Annex 3 – Charges (*Optional*)

Not Used

VI.

Annex 4 – Supplier Tender (*Optional*)

Not Used

VII. [Annex 5 – Optional IPR Clauses] (*Optional*)

Not Used