

1. SHORT FORM CONTRACT FOR THE SUPPLY OF SERVICES

I. Index

I.	Index	1
II.	Cover Letter	3
III.	Order Form	5
IV.	Short form Terms (“Conditions”)	10
1	Definitions used in the Contract	12
2	Understanding the Contract	22
3	How the Contract works	23
4	What needs to be delivered	24
5	Pricing and payments	26
6	The Buyer's obligations to the Supplier	26
7	Record keeping and reporting	27
8	Supplier Staff	28
9	Rights and protection	29
10	Intellectual Property Rights (“IPRs”)	30
11	Ending the contract	32
12	How much you can be held responsible for	34
13	Obeying the Law	38
14	Data Protection and Security	39
15	What you must keep confidential	45
16	When you can share information	46
17	Insurance	47
18	Relationships created by the contract	48
22	Giving up contract rights	48
23	Transferring responsibilities	48
24	Supply Chain	49
25	Changing the contract	50
26	How to communicate about the contract	50
27	Dealing with claims	51
28	Preventing fraud, bribery and corruption	51
29	Equality, diversity and human rights	52
30	Health and safety	52

Infected Blood

Compensation Authority



31	Environment and sustainability	53
32	Tax	53
33	Conflict of interest	54
34	Reporting a breach of the contract	54
35	Further Assurances	54
36	Resolving disputes	55
37	Which law applies	56
V.	Annex 1 – Processing Personal Data	58
VI.	Annex 2 – Specification	67
VII.	Annex 3 – Charges	70
VIII.	Annex 4 – Supplier Tender	71
IX.	Annex 5 – IPR Clauses	82
X.	Annex 6 – Non-Disclosure Agreement	86
XI.	Annex 7 – Security Management	88

II. Cover Letter

Wessex Translations Limited
Barn 500, The Grange,
Romsey Road,
Michelmersh,
Romsey, Hampshire,
SO51 0AE, UK

Attn: **REDACTED TEXT under FOIA Section 40, Personal Information.**

By email to: **REDACTED TEXT under FOIA Section 40, Personal Information.**

Date: 20th October 2025

Our ref: IBCA/P11662

Dear **REDACTED TEXT under FOIA Section 40, Personal Information.**

Following your proposal for the supply of Language Services including Translation and Interpretation Services to the Infected Blood Compensation Authority, we are pleased to confirm our intention to award this Contract to you based on the terms attached. Please note that the Contract is being awarded on a non-exclusive basis and we may appoint other suppliers to deliver similar services if required. There is no guarantee as to the volume of work which may arise under this Contract.

The attached Order Form, Contract Conditions and the Annexes set out the terms of the Contract between The Infected Blood Compensation Authority and Wessex Translations Limited for the provision of the Services set out in the Order Form.

We look forward to forging a successful working relationship resulting in a smooth and successful delivery of the Services.

Please confirm your acceptance of this Contract by signing the Order Form and returning it to me: **REDACTED TEXT under FOIA Section 40, Personal Information** and we would bring to your attention the initial supplier on-boarding requirements set out in Annex 2 to the Contract.

Infected Blood
Compensation Authority

The logo for the Infected Blood Compensation Authority features the text "Infected Blood" in a large, bold, black font, with "Compensation Authority" in a smaller, black font below it. A green horizontal line is positioned below the text, with a solid green circle centered on the line.

We will then arrange for the Order Form to be countersigned which will create a binding contract between us. Please remember to include the reference number(s) above in any future communications relating to this Contract.

Yours faithfully,

REDACTED TEXT under FOIA Section 40, Personal Information.

III. Order Form

1. Contract Reference	IBCA/P11662	
2. Buyer	The Infected Blood Compensation Authority, Block 7 Benton Park View, Longbenton, Newcastle Upon Tyne, NE98 1ZZ, 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	Wessex Translations Limited Barn 500, The Grange, Romsey Road, Michelmersh, Romsey, Hampshire, SO51 0AE, UK and registration number 04167127	
4. The Contract	This Contract between the Buyer and the Supplier is for the supply of Deliverables. The Supplier shall supply the Deliverables described below on the terms set out in this Order Form and the attached contract conditions (“ Conditions ”) and Annexes. Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in the Conditions.	
5. Deliverables	Services	The Services as described in Annex 2 -Specification are: <ul style="list-style-type: none"> • To be performed remotely and from Supplier premises at Barn 500, The Grange, Romsey Road, Romsey, Hampshire, SO51 0AE. • Date(s) of Delivery: Monday-Friday, excluding Bank holidays. Out of hours to be agreed with the Buyer.
6. Specification	The specification of the Deliverables is as set out in Annex 2 – Specification	

Infected Blood
Compensation Authority

7. Contract Start Date	20/10/2025
8. Contract Expiry Date	19/10/2026
9. Extension Period	The Buyer may extend the Contract for a period of up to 24 Months by giving not less than 10 Working Days notice in writing to the Supplier prior to the Expiry Date. The Conditions of the Contract shall apply throughout any such extended period.
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. Intellectual Property Rights (“IPR”) Clauses	The IPR Clauses shall be set out in Annex 5 – IPR Clauses.
12. Charges	The Charges for the Deliverables shall be as set out in Annex 3 – Charges
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>Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.</p> <p>All invoices must be sent, quoting a valid Purchase Order Number (PO Number) and any other relevant details, to: Invoices should be submitted to:</p> <p>REDACTED TEXT under FOIA Section 40, Personal Information.</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>Payments will be made via BACS.</p> <p>If you have a query regarding an outstanding payment please contact our Accounts Payable team either by email to: REDACTED TEXT under FOIA Section 40, Personal Information between 09:00-17:00 Monday to Friday.</p>
<p>14. Data Protection Liability Cap</p>	<p>In accordance with clause 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. of the Conditions, the Supplier’s total aggregate liability under clause indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation. of the Conditions is no more than the Data Protection Liability Cap, REDACTED TEXT under FOIA Section 43(2), Commercial Interests.</p>
<p>15. Progress Meetings and Progress Reports</p>	<ul style="list-style-type: none"> ● The Supplier shall attend progress meetings with the Buyer every month. ● The Supplier shall provide the Buyer with progress reports every month. specifically to include KPIs, Milestone and Deliverables completed, supply chain visibility, Charges and quality measures employed to deliver the contract.
<p>16. Buyer Authorised Representative(s)</p>	<p>For general liaison your contact will continue to be: REDACTED TEXT under FOIA Section 40, Personal Information or, in their absence, REDACTED TEXT under FOIA Section 40, Personal Information</p>
<p>17. Supplier Authorised Representative(s)</p>	<p>For general liaison your contact will continue to be REDACTED TEXT under FOIA Section 40, Personal Information</p>

	<p>or, in their absence,</p> <p>REDACTED TEXT under FOIA Section 40, Personal Information</p>															
<p>18. Address for notices</p>	<p>REDACTED TEXT under FOIA Section 40, Personal Information</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <p>Block 7 Benton Park View, Longbenton, Newcastle Upon Tyne, NE98 1ZZ,</p> </td> <td style="width: 50%; vertical-align: top;"> <p>Barn 500, The Grange, Romsey Road, Michelmersh, Romsey, Hampshire, SO51 0AE,UK</p> </td> </tr> </table> <p>REDACTED TEXT under FOIA Section 40, Personal Information</p>	<p>Block 7 Benton Park View, Longbenton, Newcastle Upon Tyne, NE98 1ZZ,</p>	<p>Barn 500, The Grange, Romsey Road, Michelmersh, Romsey, Hampshire, SO51 0AE,UK</p>													
<p>Block 7 Benton Park View, Longbenton, Newcastle Upon Tyne, NE98 1ZZ,</p>	<p>Barn 500, The Grange, Romsey Road, Michelmersh, Romsey, Hampshire, SO51 0AE,UK</p>															
<p>19. Key Staff</p>	<table style="width: 100%; border: none;"> <thead> <tr> <th style="text-align: left;">Key Staff Role:</th> <th style="text-align: left;">Key Staff Name</th> <th style="text-align: left;">Contact Details:</th> </tr> </thead> <tbody> <tr> <td>Director</td> <td>REDACTED TEXT under FOIA Section 40, Personal Information</td> <td></td> </tr> <tr> <td>Production Manager</td> <td>REDACTED TEXT under FOIA Section 40, Personal Information</td> <td></td> </tr> <tr> <td>Project Manager</td> <td>REDACTED TEXT under FOIA Section 40, Personal Information</td> <td></td> </tr> <tr> <td>Interpreting Manager</td> <td>REDACTED TEXT under FOIA Section 40, Personal Information</td> <td></td> </tr> </tbody> </table>	Key Staff Role:	Key Staff Name	Contact Details:	Director	REDACTED TEXT under FOIA Section 40, Personal Information		Production Manager	REDACTED TEXT under FOIA Section 40, Personal Information		Project Manager	REDACTED TEXT under FOIA Section 40, Personal Information		Interpreting Manager	REDACTED TEXT under FOIA Section 40, Personal Information	
Key Staff Role:	Key Staff Name	Contact Details:														
Director	REDACTED TEXT under FOIA Section 40, Personal Information															
Production Manager	REDACTED TEXT under FOIA Section 40, Personal Information															
Project Manager	REDACTED TEXT under FOIA Section 40, Personal Information															
Interpreting Manager	REDACTED TEXT under FOIA Section 40, Personal Information															
<p>20. Procedures and Policies</p>	<p>For the purposes of the Contract the Supplier shall follow the procedures detailed as below:</p> <ol style="list-style-type: none"> 1) The Supplier shall ensure its supply chain including specialised freelance translators at least two years' full-time professional translating experience, regardless of their qualifications. 2) The Supplier shall ensure, wherever possible, the translators should also be members of one of the industry's professional bodies (ITI, ATC or CloL). 															

	<ol style="list-style-type: none"> 3) The Supplier shall ensure that all translators meet the requirements of ISO 17100 on translator professional competences and qualifications. 4) The Supplier shall ensure that all translators have undergone a QA and QC assessment. 5) The Supplier shall ensure that all translators are to be UK-based. 6) The Supplier shall ensure that there is an IBCA specific Non-Disclosure Agreement in place between the Supplier and its supply chain including freelance translators to reinforce the confidential nature of IBCA's work as set-out in Annex 7.. 7) The Supplier shall ensure that Interpreters are NRPSI registered or equivalent. https://www.nrpsi.org.uk/about-us.html and that the Supplier shall ensure that all interpreters must meet the standards that are set for education, training and practice in public service and are subject to the NRPSI Code of Professional Conduct. 8) The Supplier's inhouse Quality Control and Quality assurance teams will ensure that additional security measures are implemented prior to delivering the translation services for the Buyer as set-out in Annex 4 - Supplier Tender. 9) The Supplier shall adhere to the Security policy and standards as set out in Annex 7 - Security Management.
<p>21. Special Terms</p>	<p>Special Term 1 -</p> <p>Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than REDACTED TEXT under FOIA Section 43(2), Commercial Interests Charges paid or payable to the Supplier.</p> <p>Special Term 2 -</p> <p>Modern Slavery: The Supplier shall comply with any request by the Buyer to complete the Modern Slavery Assessment Tool, which can be found online at: https://supplierregistration.cabinetoffice.gov.uk/msat, within sixty (60) days of such request.</p> <p>Special Term 3 -</p> <p>The Supplier must have the following accreditations:</p> <ol style="list-style-type: none"> 1) ISO Certification: ISO 9001:2015.

	<p>2) Cyber Essentials.</p> <p>3) Association of Translation Companies (ATC).</p> <p>4) Corporate membership of the Institute of Translation and Interpreting (ITI).</p> <p>Special Term 4 - Indemnity</p> <p>The Supplier indemnifies the Buyer from any liability arising from legal claims made by any of IBCA's claimants where the sole cause is down to inaccurate translation or interpretations services provided by the Supplier and its supply chain.</p>
<p>22. Incorporated Terms</p>	<p>The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies:</p> <p>(a) The cover letter from the Buyer to the Supplier dated 20th October 2025.</p> <p>(b) This Order Form</p> <p>(c) Any Special Terms (see row Special Terms (Special Terms) in this Order Form)</p> <p>(d) Conditions (as they may be amended by Annex 5 – IPR Clauses)</p> <p>(e) The following Annexes in equal order of precedence:</p> <ul style="list-style-type: none"> i. Annex 1 – Processing Personal Data ii. Annex 2 – Specification iii. Annex 3 – Charges iv. Annex 4 – Supplier Tender unless any part of the Tender offers a better commercial position for the Buyer (as decided by the Buyer, in its absolute discretion), in which case that part of the Tender will take precedence over the documents above. v. Annex 5 - IPR Clauses vi. Annex 6 - Non-Disclosure Agreement vii. Annex 7 - Security Management

Signed for and on behalf of the Supplier	Signed for and on behalf of the Buyer acting on behalf of the Infected Blood Compensation Authority
--	---

Infected Blood
Compensation Authority



Name: REDACTED TEXT under FOIA Section 40, Personal Information	Name: REDACTED TEXT under FOIA Section 40, Personal Information
Date: 20/10/2025	Date: 21st October 2025
Signature: REDACTED TEXT under FOIA Section 40, Personal Information	Signature: REDACTED TEXT under FOIA Section 40, Personal Information

IV. 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 What needs to be delivered to Reporting a breach of the contract (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;

Infected Blood

Compensation Authority



	<p>(g) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Contract;</p> <p>(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;</p> <p>(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;</p>
“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”	<p>all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which</p> <p>(a) is known by the receiving Party to be confidential;</p> <p>(b) is marked as or stated to be confidential; or</p> <p>(c) ought reasonably to be considered by the receiving Party to be confidential;</p>
“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;

Infected Blood
Compensation Authority



“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 Data Protection Liability Cap 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;

Infected Blood
Compensation Authority



“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 Goods clauses. “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”	any event, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from: (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

Infected Blood

Compensation Authority



	<p>delay the Affected Party from performing its obligations under the Contract;</p> <p>(b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare;</p> <p>(c) acts of a Crown Body, local government or regulatory bodies;</p> <p>(d) fire, flood or any disaster; or</p> <p>(e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available</p> <p>but excluding:</p> <p>(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;</p> <p>(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</p> <p>(c) any failure of delay caused by a lack of funds,</p> <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”	<p>(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:</p> <p>(i) are supplied to the Supplier by or on behalf of the Buyer; or</p>

	<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 Joint Controller Agreement (Optional) Joint Controller Agreement (Optional) 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”	technical and organisational measures which must take account of: <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; 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;

Infected Blood
Compensation Authority



“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”	<p>any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party:</p> <ul style="list-style-type: none"> (a) provides the Deliverables (or any part of them);

	<p>(b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or</p> <p>(c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);</p>
“Subcontractor”	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
“Subprocessor”	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 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form. 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) (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 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles) as updated from time to time except for:</p>

	<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</p> <p>(b) Confidential Information;</p>
“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, the tender in Annex 4 – Supplier Tender (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 (Not Applicable)

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 Goods clauses. 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 When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination). Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause Resolving disputes.

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 Ending the contract;
 - 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 If Supplier fails to comply with the Contract as a result of a Buyer Cause: 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 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 8 of Part B Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data (if used), all of the following apply: 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 a 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 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. and clause The Supplier warrants and represents that: 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 Intellectual Property Rights ("IPRs").

- 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 What you must keep confidential (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 Intellectual Property Rights ("IPRs") 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 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: 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 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, all of the following apply: 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 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;; 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 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:
- (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 its terminated clause 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: 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 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 8 of Part B Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data (if used), all of the following apply: 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 the Buyer's payment obligations under the terminated Contract stop immediately; to 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. apply.

11.5 What happens if the Contract ends

11.5.1 Where the Buyer terminates the Contract under clause 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., When the Buyer can end the Contract, 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., immediately terminate the Contract and the consequences of termination in Clause 11.5.1 shall apply. 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: Definitions used in the Contract, 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., Pricing and payments, Record keeping and reporting, 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., Intellectual Property Rights (“IPRs”), What happens if the Contract ends, How much you can be held responsible for, Data Protection and Security, What you must keep confidential, When you can share information, Invalid parts of the contract, Other people's rights in the contract, 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., Resolving disputes and Which law applies 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 Ending the Contract without a reason or the Supplier terminates the Contract under clause When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination) or The Supplier can terminate the Contract novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event.:

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 the Buyer's payment obligations under the terminated Contract stop immediately; to 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. apply.

11.6.3 The Supplier also has the right to terminate the Contract in accordance with Clauses 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. and The Supplier can terminate the Contract novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event..

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 Changing the contract) any necessary variation required by clause Partially ending and suspending the Contract, 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 Ending the Contract without

11.7.3.3

11.7.3.4 a reason.

11.7.4 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause Partially ending and suspending the Contract.

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 **REDACTED TEXT under FOIA Section 43(2), Commercial Interests**. Charges paid or payable to the Supplier.

12.2 No Party is liable to the other for:

Infected Blood
Compensation Authority

- 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 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than **REDACTED TEXT under FOIA Section 43(2), Commercial Interests.** of the Charges paid or payable to the Supplier., 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 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than **REDACTED TEXT under FOIA Section 43(2), Commercial Interests.** of the Charges paid or payable to the Supplier., the Supplier does not limit or exclude its liability for any indemnity given under clauses 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., non-payment by the Supplier of any tax or National Insurance., 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., or 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..
- 12.5 In spite of clause Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than **REDACTED TEXT under FOIA Section 43(2), Commercial Interests.** of the Charges paid or payable to the Supplier., the Buyer does not limit or exclude its liability for any indemnity given under clause 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..

- 12.6 Notwithstanding clause Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than **REDACTED TEXT under FOIA Section 43(2), Commercial Interests.** of the Charges paid or payable to the Supplier., but subject to clauses Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than **REDACTED TEXT under FOIA Section 43(2), Commercial Interests.** of the Charges paid or payable to the Supplier. and In spite of clause 12.1, neither Party limits or excludes any of the following:., the Supplier's total aggregate liability under clause indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation. 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) 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

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

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 The Supplier, in connection with provision of the Deliverables: and clauses Dealing with claims to Reporting a breach of the contract.

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.

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 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both: 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 Data Protection and Security 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”,
 - 1. in respect of certain Personal Data under the Contract and shall specify in Authorised Processing Template 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 Authorised Processing Template 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 in relation to any Personal Data processed under this Contract:
- 14.9.4.1 process that Personal Data only in accordance with Authorised Processing Template 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 Authorised Processing Template 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 Data Protection and Security;
 - (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,

1. 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 The Processor must notify the Controller immediately if it: 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 The Processor must notify the Controller immediately if it:. 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 Data Protection and Security. 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 Data Protection and Security 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 (Not applicable)

- 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 Joint Controller Agreement (Optional) Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data.

14.11 Independent Controllers of Personal Data (Not Applicable)

- 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 Independent Controllers (Optional) 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 Each Party must:, 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 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. and When you can share information.
- 15.5 For the purposes of clauses 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: to The Buyer may disclose Confidential Information in any of the following cases: references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause What you must keep confidential.
- 15.6 Transparency Information, and Information which is exempt from disclosure by clause When you can share information 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 When you can share information. 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 the Buyer's payment obligations under the terminated Contract stop immediately; to 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. shall apply.

20.4 Where a Party terminates under clause 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.:

20.4.1 each Party must cover its own losses; and

20.4.2 clauses the Buyer's payment obligations under the terminated Contract stop immediately; to 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. 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 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. 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 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. 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 When the Buyer can end the Contract;
 - 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 The Supplier shall not: 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 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., 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 The Supplier shall not: 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 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 8 of Part B Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data (if used), all of the following apply: 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 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:, 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 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: 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 the Buyer's payment obligations under the terminated Contract stop immediately; to 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. 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 The Supplier, in connection with provision of the Deliverables:, or clauses Dealing with claims to Conflict of interest.
- 34.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 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. 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 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. : to 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..
- 36.3 Unless the Buyer refers the dispute to arbitration using clause 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., 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 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. ∴, 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 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..
- 36.6 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.

V. Annex 1 – Processing Personal Data

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:

REDACTED TEXT under FOIA Section 40, Personal Information.

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

REDACTED TEXT under FOIA Section 40, Personal Information.

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	<p>Translation and Interpretation services</p> <p>Infected Blood Compensation Authority (IBCA) – Data Controller</p> <p>Wessex Translations Limited – Data Processor</p>
Subject matter of the processing	<p>The processing is needed to ensure that the Processor can effectively deliver the contract to provide translation and interpretation services.</p> <p>The subject matter of the processing is the review of medical records containing personal and special category data about victims of infected blood.</p> <p>This involves the receipt of medical (and supporting) documents from the IBCA which have been written in a language other than English and data presented during live interpretation services. The Supplier will be translating the documents into English on behalf of IBCA as well as interpreting to and from a foreign language in an interpretation scenario.</p>

Duration of the processing	Commencing 20th October 2025, for a term of one (1) year: followed by two (2) further term extensions of one (1) year up to a maximum total duration of three (3) years.
Nature and purposes of the processing	<p>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose includes supporting the IBCA to enable processing of medical claims, by translating medical records (that are currently held not in English language) into English.</p> <p>The Supplier will provide access to an external secure FTP portal that will allow the Buyer to upload the identified documents. The Supplier will use the services of their supply chain, independent translators and interpreters (SubProcessor(s)).</p> <p>For interpretation, the buyer will provide the platform and environment to enable interpretation services to be delivered.</p> <p>Access controls will be in place at the secure FTP portal level, to provide restricted access to documents by identified sub-contractors (SubProcessors) - additional controls will be in place to restrict printing, downloading, deleting.</p>
Type of Personal Data being processed	<p>Medical records will include:</p> <p>Name, address, date of birth, gender, contact details (phone / email), health data e.g. medical reports detailing medical conditions and procedures, which may include:</p> <ul style="list-style-type: none"> · <i>blood test results and dates</i> · <i>scan results and dates</i> · <i>emails/letters to patient advising of a diagnosis</i> · <i>emails/letters internally between clinicians/hospitals/GPs confirming diagnosis</i>

Infected Blood

Compensation Authority



	<ul style="list-style-type: none"> · <i>evidence of blood transfusion and the dates</i> · <i>evidence of operation where they may have received a blood transfusion and dates</i> · <i>evidence of treatment and dates</i>
Categories of Data Subject	<p>Claimants, Children, Members of the public, Medical staff, Legal representatives, Public authority staff</p> <p>(UK and/or overseas)</p>
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	<p>The IBCA will be responsible for providing clear instructions to the Supplier on the destruction or cease of provision of data for the service.</p> <p>IBCA will be given access controls allowing for deletion of documents from the portal, once a document has been marked as COMPLETE.</p> <p>Once a file has been marked as translation COMPLETE and downloaded by IBCA, the supplier must delete the document after 90 days.</p> <p>The Supplier will also delete the document(s) from the recycle bin.</p>
Locations at which the Supplier and/or its Subcontractors process Personal Data under this Contract and International transfers and legal gateway	<p>N/A</p> <p>Whilst processing, the Supplier will host the data in the UK. Any authorised SubProcessors will access the data from within the Supplier external collaboration site, meaning the data will remain at all times in a single data repository.</p> <p>All SubProcessors will be based in the UK.</p>

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	To be agreed with the Buyer post contract award.
--	--

38 DATA PROTECTION BREACH

38.1 Without prejudice to Paragraph Each Party shall use best endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Data Loss Event which is the fault of that Party as if it was that Party’s own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Data Loss Event, including providing the other Party, as soon as possible and within 48 hours of the Data Loss Event relating to the Data Loss Event, in particular: of this Joint Controller Agreement (Optional) Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Data Loss Event or circumstances that are likely to give rise to a Data Loss Event, providing the other Party and its advisors with:

- 38.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Event under the Data Protection Legislation;
- 38.1.2 all reasonable assistance, including:
 - 38.1.2.1 co-operation with the other Party and the Information Commissioner investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - 38.1.2.2 co-operation with the other Party including using such best endeavours as are directed by the Buyer to assist in the investigation, mitigation and remediation of a Data Loss Event;

- 38.1.2.3 co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or
- 38.1.2.4 providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Data Loss Event, with complete information relating to the Data Loss Event, including the information set out in Paragraph Each Party shall use best endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Data Loss Event which is the fault of that Party as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Data Loss Event, including providing the other Party, as soon as possible and within 48 hours of the Data Loss Event relating to the Data Loss Event, in particular: of this Joint Controller Agreement (Optional) Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data;.

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

- 38.2.1 the nature of the Data Loss Event;
- 38.2.2 the nature of Personal Data affected;
- 38.2.3 the categories and number of Data Subjects concerned;
- 38.2.4 the name and contact details of the Party's Data Protection Officer or other relevant contact from whom more information may be obtained;
- 38.2.5 measures taken or proposed to be taken to address the Data Loss Event; and
- 38.2.6 a description of the likely consequences of the Data Loss Event.

39 **AUDIT**

39.1 The Supplier shall permit:

39.1.1 the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this of this Joint Controller Agreement (Optional) Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data; and the Data Protection Legislation; and/or

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

39.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph The Supplier shall permit: of this Joint Controller Agreement (Optional) Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data in lieu of conducting such an audit, assessment or inspection.

40 IMPACT ASSESSMENTS

40.1 The Parties shall:

40.1.1 provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures); and

40.1.2 maintain full and complete records of all processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

41 ICO GUIDANCE

41.1 The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Crown Body.

42 LIABILITIES FOR DATA PROTECTION BREACH

- 42.1 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:
- 42.1.1 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;
 - 42.1.2 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
 - 42.1.3 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 Resolving disputes of the Conditions (Resolving disputes).
- 42.2 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.

- 42.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the “**Claim Losses**”):
- 42.3.1 if the Buyer is responsible for the relevant Data Loss Event, then the Buyer shall be responsible for the Claim Losses;
 - 42.3.2 if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and
 - 42.3.3 if responsibility for the relevant Data Loss Event is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.
- 42.4 Nothing in either Paragraph 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. or Paragraph In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the “Claim Losses”): of this Joint Controller Agreement (Optional) 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.

43 TERMINATION

- 43.1 If the Supplier is in Material Breach under any of its obligations under this of this Joint Controller Agreement (Optional) 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 Ending the contract of the Conditions (Ending the contract).

44 SUB-PROCESSING

- 44.1 In respect of any processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

- 44.1.1 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
- 44.1.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

45 DATA RETENTION

- 45.1 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.

VI. Annex 2 – Specification

BACKGROUND

In the c.12 months since its inception, Infected Blood Compensation Authority (IBCA) has made massive progress towards its objective to stand up a fully operational Arms Length Body from the 1st of October.

The ongoing expansion of IBCA's Compensation Service and payments made to over 2500 claimants so far, there is an ongoing requirement for processing claims for non-english speaking claimants This service will require to be fulfilled via telephone (spoken telephone and spoken visual video), Translation of written documents such as medical records.

IBCA have received small numbers of non-English documents, including medical records, that are key to understanding claims for compensation, and as the organisation continues to process further claims for compensation, the number of claims that require translation or interpretation are expected to grow.

IBCA requires a supplier to undertake translation of these documents into English, sufficient to enable accurate decisions to be made on compensation under the terms of the Infected Blood Compensation Scheme.

There is also a potential requirement for communications from IBCA to be translated from English into another language.

The Supplier will need to work with IBCA Operations, including Claim Managers, as well as Clinical Advisors to enable decisions to be made on compensation.

The Supplier must ensure that all translators and interpreters employed to deliver this contract are to be UK-based ONLY.

DESCRIPTION OF REQUIREMENT

The following areas are in scope:

1. Translation of documents into English language on request
 - Documents likely to include medical records, test results and specialist medical terminology. The Supplier must be able to accurately translate these into equivalent English terminology.
 - Source documents may be both handwritten as well as typed.
 - Each request will include one or more documents relating to an individual
 - On request, provide a precis or summary of the documents relating to the person, including key facts or any conflicting information

- Upon request, attend calls including IBCA and a clinical advisor to assist understanding of the original documents in the context of the claim.
2. Translation of communications from English into a non-English language
 - Outbound communications for IBCA to be translated into target language, so that the person making the claim can fully understand the required details of their claim, and enabling them to make informed decisions.
 3. Interpreting between English and a non-English language
 - Interpreting of conversations between IBCA and a person making a claim, through phone calls or videos calls
 - Interpreting required only during office hours, 08:00 to 18:00, Monday to Friday, no bank holidays.
 - Time to book an interpreter within 5 Working Days.
 4. Volumes
 - IBCA does not have any accurate forecasts of volumes.
 - Best guide might be where IBCA have international payments - still need Wales, Northern Ireland and Scotland data.

Key Performance Indicators /Service Levels

KPI/SLA Area	SLA Description	Target
Confirmation of receipt of enquiry	4 working hours	100%
Delivery of standard 1 page	4-5 working days	100%
Delivery of standard 3 pages	4-5 working days	100%
Delivery of standard 10 pages	7-9 working days	100%
Delivery of standard 30 pages	10-15 working days	100%
Quality	Quality controls	100% of translations undergo Wessex Translation's in-house quality controls

Key Milestones and Deliverables

Milestone / Deliverable	Description	Timeframe or Delivery Date
1.	Setting up the secure FTP portal	Within 3 Working Days from Contract Start Date
2.	On-boarding completed	Within 5 Working Days from Contract Start Date

On-boarding Requirements

- Independent Translators and Interpreter to complete Supplier application forms.
- Quality assessment and test requirements completed.
- NDA to be signed with additional measures included as per Buyer requirements.
- Secure FTP Portal to be set-up.
- Kick-off meeting with Buyer to be arranged within 5 Working Days of Contract Start Date.
- Enquiry process : The Buyer to submit project enquiry to **REDACTED TEXT under FOIA Section 40, Personal Information** with details as below:

An enquiry can be sent by email, an example of requested details needed:

Contact name	
Contact email	
Contact telephone number	
Language requirement	I.e. explain what the documents are, the language they are in (if known) and the language they should be translated into.
Delivery timescales	Is there a specific must have deadline or expected time-frame?
Specific Instructions	Unless specified differently, full and complete translations will be provided. If there is any specific information needed, please identify.

VII. Annex 3 – Charges

A) Translation – allows for translation plus revision by a second linguist, medical content and in handwritten format.

Per 1000 words	Into English	From English
French, German, Italian, Spanish, Dutch, Portuguese	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
Danish, Finnish, Norwegian, Swedish	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
Albanian, Bulgarian, Czech, Estonian, Hungarian, Latvian, Polish, Romanian, Russian, Slovak, Slovenian	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
Greek, Turkish, Welsh	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
Arabic, Farsi, Bengali, Gujarati, Hindi, Punjabi, Urdu	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
Chinese, Japanese, Korean, Vietnamese	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.

B) Interpreting – Teams (online)

All languages	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
---------------	--

Interpreting – Face to Face – will vary depending on location and travel arrangements

All languages	REDACTED TEXT under FOIA Section 43(2), Commercial Interests.
---------------	--

VIII. Annex 4 – Supplier Tender

REDACTED TEXT under FOIA Section 43(2), Commercial Interests.

IX. Annex 5 – IPR Clauses

**Part A Buyer ownership with limited Supplier rights to exploit New IPR for the purposes
of the current Contract**

46 INTELLECTUAL PROPERTY RIGHTS (“IPRs”)

- 46.1 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:
- 46.1.1 receive and use the Deliverables; and
 - 46.1.2 use the New IPR.
2. The termination or expiry of the Contract does not terminate any licence granted under this clause 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:.
- 46.2 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 for the purpose of fulfilling its obligations during the Term. 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 What you must keep confidential (What you must keep confidential).
- 46.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.
- 46.4 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.
- 46.5 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 clause Intellectual Property Rights (“IPRs”) or otherwise agreed in writing.
- 46.6 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.
- 46.7 If an IPR Claim is made or anticipated the Supplier must at its own option and expense, either:

- 46.7.1 obtain for the Buyer the rights in clause 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: without infringing any third party intellectual property rights; and
 - 46.7.2 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.
- 46.8 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 clause Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 8 of Part B Joint Controller Agreement (Optional) of Annex 1 – Processing Personal Data (if used), all of the following apply: shall apply.
- 46.9 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:
- 46.9.1 the Buyer gives its approval to do so; and
 - 46.9.2 one of the following conditions applies:
 - 46.9.2.1 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 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; or
 - 46.9.2.2 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 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:
 - (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

46.9.2.3 the Buyer approves in writing, with reference to the acts authorised and the specific intellectual property rights involved.

- 46.10 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.
- 46.11 Subject to clause 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., the Supplier agrees that the Buyer may at its sole discretion publish under Open Licence all or part of the New IPR Items and the Supplier warrants that the New IPR Items are suitable for release under Open Licence and that the publication of the New IPR Items under Open Licence will not infringe the rights of any third party and will not harm any Third Party or the Buyer.
- 46.12 The Supplier will supply any or all New IPR Items in a format suitable for publication under Open Licence (“**the Open Licence Publication Material**”) within 30 days of written request from the Buyer (“**Buyer Open Licence Request**”). Where any Supplier Existing IPR is included in the Open Licence Publication Material, this will become Open Licence material.
- 46.13 The Supplier may within 15 days of a Buyer Open Licence Request under clause The Supplier will supply any or all New IPR Items in a format suitable for publication under Open Licence (“the Open Licence Publication Material”) within 30 days of written request from the Buyer (“Buyer Open Licence Request”). Where any Supplier Existing IPR is included in the Open Licence Publication Material, this will become Open Licence material., request in writing that the Buyer excludes all or part of:
- 46.13.1 the New IPR; or

46.13.2 Supplier Existing IPR or Third Party IPR that would otherwise be included in the Open Licence Publication Material supplied to the Buyer pursuant to clause The Supplier will supply any or all New IPR Items in a format suitable for publication under Open Licence (“the Open Licence Publication Material”) within 30 days of written request from the Buyer (“Buyer Open Licence Request”). Where any Supplier Existing IPR is included in the Open Licence Publication Material, this will become Open Licence material.

46.13.3 from Open Licence publication.

46.14 Any decision to approve any such request from the Supplier pursuant to clause The Supplier may within 15 days of a Buyer Open Licence Request under clause 10.12, request in writing that the Buyer excludes all or part of: shall be at the Buyer’s sole discretion, not to be unreasonably withheld, delayed or conditioned.

46.15 Subject to clause How much you can be held responsible for, the Buyer will not be liable in the event that any Supplier Existing IPR or Third Party IPR is included in the Open Licence Publication Material published by the Buyer.

X. Annex 6 – Non-Disclosure Agreement

This NDA needs to be between Wessex Translations and its supply chain, independent translators and linguists employed for the delivery of this contract. .

For the attention of XYZ

Date : xx/xx/2025

CONFIDENTIALITY AGREEMENT

As part of our commitment to IBCA we ask all part and full-time staff and external consultants and suppliers working for Wessex Translations to sign this agreement, in order to reinforce the confidential nature of our work.

Wessex Translations Limited undertakes work of a highly sensitive nature on behalf of IBCA, relating to commercially sensitive information and contract. You are therefore asked to read the following confidentiality agreement carefully before signing it:

When undertaking work for Wessex Translations in whatever form (translation, interpreting, quality control editing, project management etc.), we undertake to maintain strict confidentiality as to the identity of end clients, their businesses and their materials, as well as the identity of Wessex Translations' suppliers and any information relating to them. We will not transmit or divulge any of the materials supplied to us as part of work undertaken, or any of the information therein contained, or any information regarding the names of, or financial or commercial information concerning Wessex Translations' end clients, howsoever gained in the course of my work, to any third party. Moreover, if work is to be taken home, I will not leave information unattended in my office, nor retain either hard or soft copies of any text without your permission.

I will also maintain strict confidentiality as to the business of Wessex Translations, its systems, equipment, financial, commercial or other company information, howsoever gained in the course of my work, to any third party, unless already in the public domain.

Signed: _____

Date: _____

XI. Annex 7 – Security Management

1 SUPPLIER OBLIGATIONS

Core requirements

- 1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 8.
- 1.2 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Certifications (see Paragraph 4)		
The Supplier must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	<input checked="" type="checkbox"/>
	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	<input checked="" type="checkbox"/>
	No certification required	<input type="checkbox"/>
Subcontractors that Handle Government Data must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	<input type="checkbox"/>
	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	<input type="checkbox"/>
	No certification required	<input checked="" type="checkbox"/>
Locations (see Paragraph 5)		
The Supplier and Subcontractors may store, access or Handle Government Data in:	the United Kingdom only	<input checked="" type="checkbox"/>



	a location permitted by and in accordance with any regulations for the time being in force made under 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>
Staff Vetting Procedure (see Paragraph 6)		
The Buyer requires a Staff Vetting Procedure other than BPSS		<input type="checkbox"/>

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding Paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Buyer Security Policies (see Paragraph 10)	
The Buyer requires the Supplier to comply with the following policies relating to security management: <ul style="list-style-type: none"> • [List Buyer security policies with which the Supplier and Sub-contractors must comply]. 	<input type="checkbox"/>
Security testing (see Paragraph 11)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	<input type="checkbox"/>
Cloud Security Principles (see Paragraph 12)	

The Supplier must assess the Supplier System against the Cloud Security Principles	<input type="checkbox"/>
Record keeping (see Paragraph 13)	
The Supplier must keep records relating to Subcontractors, Sites, Third-Party Tools and third parties	<input checked="" type="checkbox"/>
Encryption (see Paragraph 14)	
The Supplier must encrypt Government Data while at rest or in transit	<input checked="" type="checkbox"/>
Protective Monitoring System (see Paragraph 15)	
The Supplier must implement an effective Protective Monitoring System	<input type="checkbox"/>
Patching (see Paragraph 16)	
The Supplier must patch vulnerabilities in the Supplier System promptly	<input checked="" type="checkbox"/>
Malware protection (see Paragraph 17)	
The Supplier must use appropriate Anti-virus Software	<input checked="" type="checkbox"/>
End-User Devices (see Paragraph 18)	
The Supplier must manage End-User Devices appropriately	<input checked="" type="checkbox"/>
Vulnerability scanning (see Paragraph 19)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	<input checked="" type="checkbox"/>
Access control (see Paragraph 20)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	<input checked="" type="checkbox"/>

Remote Working (see Paragraph 21)	
The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	<input type="checkbox"/>
Backup and recovery of Government Data (see Paragraph 22)	
The Supplier must have in place systems for the backup and recovery of Government Data	<input type="checkbox"/>
Return and deletion of Government Data (see Paragraph 23)	
The Supplier must return or delete Government Data when requested by the Buyer	<input checked="" type="checkbox"/>
Physical security (see Paragraph 24)	
The Supplier must store Government Data in physically secure locations	<input checked="" type="checkbox"/>
Security breaches (see Paragraph 25)	
The Supplier must report any Breach of Security to the Buyer promptly	<input checked="" type="checkbox"/>

2 DEFINITIONS

“Anti-virus Software”

means software that:

- (a) protects the Supplier System from the possible introduction of Malicious Software;
- (b) scans for and identifies possible Malicious Software in the Supplier System;

- (c) if Malicious Software is detected in the Supplier System, so far as possible:
 - (i) prevents the harmful effects of the Malicious Software; and
 - (ii) removes the Malicious Software from the Supplier System;

"BPSS" means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>), as that document is updated from time to time;

"Breach of Security" means the occurrence of:

- (a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;
- (b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or
- (c) any part of the Supplier System ceasing to be compliant with the required Certifications;
- (d) the installation of Malicious Software in the Supplier System;
- (e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and

- (f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:
 - (i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or
 - (ii) was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Equipment" means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;

"Buyer Security Policies" means those securities specified by the Buyer in Paragraph 1.3;

"Buyer System" means the Buyer's information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that:

- (a) is used by the Buyer or Supplier in connection with this Contract;
- (b) interfaces with the Supplier System; and/or
- (c) is necessary for the Buyer to receive the Services.

"Certifications" means one or more of the following certifications (or equivalent):

- (a) ISO/IEC 27001:2022 by a UKAS- recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and
- (b) Cyber Essentials Plus; and/or

- (c) Cyber Essentials;
- “CHECK Scheme”** means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
- “CHECK Service Provider”** means a company which, under the CHECK Scheme:
- (a) has been certified by the NCSC;
 - (b) holds “Green Light” status; and
 - (c) is authorised to provide the IT Health Check services required by Paragraph 9.2 (*Security Testing*);
- “Cloud Security Principles”** means the NCSC’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles>;
- “Contract Year”** means:
- 14.9.1 a period of 12 months commencing on the Start Date;
 - 14.9.2 thereafter a period of 12 months commencing on each anniversary of the Start Date;
- (a) with the final Contract Year ending on the expiry or termination of the Term;
- “CREST Service Provider”** means a company with an information security accreditation of a security operations centre qualification from CREST International;
- “Cyber Essentials”** means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;

- “Cyber Essentials Plus”** means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
- “Cyber Essentials Scheme”** means the Cyber Essentials scheme operated by the NCSC;
- “Developed System”** means the software or system that the Supplier is required to develop under this Contract;
- “End-User Device”** means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
- “Expected Behaviours”** means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of <https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html>;
- “Government Data”** Means any: .
- (a) data, texts, 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;
 - (b) Personal Data for which the Buyer is a, or the, Data Controller; or
 - (c) any meta-data relating to categories of data referred to in Paragraphs (a) or (b);
- that is:
- (d) supplied to the Supplier by or on behalf of the Buyer; or

(e) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract;

"Government Security Classification Policy"	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications ;
"Handle"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
"IT Health Check"	means the security testing of the Supplier System;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance ;
"Privileged User"	means a user with system administration access to the Supplier System, or substantially similar access privileges;

“Prohibition Notice”	means the meaning given to that term by Paragraph 4.4.
“Protective Monitoring System”	has the meaning given to that term by Paragraph 13.1;
“Relevant Conviction”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
“Remote Location”	means [the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for Remote Working OR a location other than a Supplier's or a Sub-contractor's Site];
“Remote Working”	means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
“Remote Working Policy”	the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working;
“Security Controls”	means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html ;
“Sites”	means any premises (including the Buyer's Premises, the Supplier's premises or third party premises): <ul style="list-style-type: none">(a) from, to or at which: <ul style="list-style-type: none">(i) the Services are (or are to be) provided; or

(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or

(b) where:

(i) any part of the Supplier System is situated; or

(ii) any physical interface with the Buyer System takes place;

"Staff Vetting Procedure" means the procedure for vetting Supplier Staff set out in Paragraph 6;

"Subcontractor Staff" means:

(a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and

(b) engaged in or likely to be engaged in:

(i) the performance or management of the Services; or

(ii) the provision of facilities or services that are necessary for the provision of the Services;

"Supplier System" means

(a) any:

(i) information assets,

(ii) IT systems,

(iii) IT services; or

(iv) Sites,

that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, or support the provision of, the Services; and

(b) the associated information management system, including all relevant:

(i) organisational structure diagrams;

(ii) controls;

(iii) policies;

(iv) practices;

(v) procedures;

(vi) processes; and

(vii) resources;

“Third-party Tool”

means any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

“UKAS-recognised Certification Body”

means:

(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or

(b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment.

PART ONE: CORE REQUIREMENTS

3 HANDLING GOVERNMENT DATA

3.1 The Supplier acknowledges that it:

- (a) must only Handle Government Data that is classified as OFFICIAL; and
- (b) must not Handle Government Data that is classified as SECRET or TOP SECRET.

3.2 The Supplier must:

- (a) not alter the classification of any Government Data.
- (b) if it becomes aware that it has Handled any Government Data classified as SECRET or TOP SECRET the Supplier must:
 - i. immediately inform the Buyer; and
 - ii. follow any instructions from the Buyer concerning the Government Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

- (a) the Expected Behaviours; and
- (b) the Security Controls.

4 CERTIFICATION REQUIREMENTS

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

(a) it; and

(b) any Subcontractor that Processes Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications):

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Subcontractor:

(a) before the Supplier or any Subcontractor Handles Government Data; and

(b) throughout the Term.

5 LOCATION

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

(a) the United Kingdom; or

(b) a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

5.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that all Subcontractors, at all times store, access or Handle Government Data only in or from the geographic areas specified by the Buyer.

5.3 The Supplier must, and must ensure that its Subcontractors store, access or Handle Government Data in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);(b) that binding agreement includes obligations on the entity in relation to security management at least as onerous as those relating to Subcontractors in this Annex;

(c) the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Process the Government Data as required by this Annex;

5.3.1 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

5.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Processing of Government Data in one or more countries or territories (a "**Prohibition Notice**").

5.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

6 STAFF VETTING

6.1 The Supplier must not allow Supplier Staff, and must ensure that Subcontractors do not allow Subcontractor Staff, to access or Handle Government Data, if that person:

(a) has not completed the Staff Vetting Procedure; or

(b) where no Staff Vetting Procedure is specified in the Order Form:

i. has not undergone the checks required for the BPSS to verify:

A. the individual's identity;

B. where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom; and

C. the individual's previous employment history; and

D. that the individual has no Relevant Convictions; and

ii. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify.

- 6.2 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Staff, it must:
- (a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
 - (b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor staff will perform as the Buyer reasonably requires; and
 - (c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contract.

7 SUPPLIER ASSURANCE LETTER

- 7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its Director confirming that, having made due and careful enquiry:
- (a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;
 - (b) it has fully complied with all requirements of this Annex; and
 - (c) all Subcontractors have complied with the requirements of this Annex with which the Supplier is required to ensure they comply;
 - (d) the Supplier considers that its security and risk mitigation procedures remain effective.

8 ASSURANCE

- 8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Annex.
- 8.2 The Supplier must provide that information and those documents:
- (a) at no cost to the Buyer;
 - (b) within 10 Working Days of a request by the Buyer;

(a) except in the case of original document, in the format and with the content and information required by the Buyer; and

(b) in the case of original document, as a full, unedited and unredacted copy.

9 USE OF SUBCONTRACTORS AND THIRD PARTIES

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Annex.

10 BUYER SECURITY POLICIES

10.1 The Supplier must comply, when it provides the Services and operates and manages the Supplier System, with all Buyer Security Policies identified in the relevant option in Paragraph 1.3.

10.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Annex, then the requirements of this Annex will prevail to the extent of that inconsistency.

11 SECURITY TESTING

11.1 The Supplier must:

(a) before Handling Government Data;

(b) at least once during each Contract Year; and

undertake the following activities:

(c) conduct security testing of the Supplier System (an “**IT Health Check**”) in accordance with Paragraph 12.2; and

(d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 12.3.

11.2 In arranging an IT Health Check, the Supplier must:

(a) use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

- (b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;
- (c) ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Process or manage Government Data; and
- (d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

11.3 The Supplier treat any vulnerabilities as follows:

(a) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

- i. if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or
- ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(a)(i) , then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(b) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

- i. if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or
- ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(c) the Supplier must remedy any vulnerabilities classified as medium in the IT Health Check report:

- iii. if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or
- iv. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

12. CLOUD SECURITY PRINCIPLES

12.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

12.2 The Supplier must assess the Supplier System against the Cloud Security Principles to assure itself that it complies with Paragraph 10.1:

- before Handling Government Data;
- at least once each Contract Year; and
- when required by the Buyer.

12.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

12.4 The Supplier must:

- (a) keep records of any assessment that it makes under Paragraph 13.2; and
- (b) provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

13. INFORMATION ABOUT SUBCONTRACTORS, SITES AND THIRD-PARTY TOOLS

13.1 The Supplier must keep the following records:

(a) for Subcontractors or third parties that store, have access to or Handle Government Data:

- v. the Subcontractor or third party's name:
 - A. legal name;
 - B. trading name (if any); and

- C. registration details (where the Subcontractor is not an individual), including:
 - (A) country of registration;
 - (B) registration number (if applicable); and
 - (C) registered address;
 - D. the Certifications held by the Subcontractor or third party;
 - E. the Sites used by the Subcontractor or third party;
 - F. the Services provided or activities undertaken by the Subcontractor or third party;
 - G. the access the Subcontractor or third party has to the Supplier System;
 - H. the Government Data Handled by the Subcontractor or third party; and
 - I. the measures the Subcontractor or third party has in place to comply with the requirements of this Annex;
- vi. for Sites from or at which Government Data is accessed or Handled:
- A. the location of the Site;
 - B. the operator of the Site, including the operator's:
 - (A) legal name;
 - (B) trading name (if any); and
 - (C) registration details (where the Subcontractor is not an individual);
 - C. the Certifications that apply to the Site;

- D. the Government Data stored at, or Handled from, the site; and
- vii. for Third-party Tools:
 - A. the name of the Third-Party Tool;
- viii. the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and
 - A. in respect of the entity providing the Third-Party Tool, its:
 - (A) full legal name;
 - (B) trading name (if any)
 - (C) country of registration;
 - (D) registration number (if applicable); and
 - (E) registered address.

13.2 The Supplier must update the records it keeps in accordance with Paragraph 14.1:

- (a) at least four times each Contract Year;
- (b) whenever a Subcontractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or
- (c) whenever required to go so by the Buyer.

13.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 14.1 to the Buyer within 10 Working Days of any request by the Buyer.

14 ENCRYPTION

14.1 The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

- when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and
- when transmitted.

15 PROTECTIVE MONITORING SYSTEM

15.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

- (a) identify and prevent any potential Breach of Security;
- (b) respond effectively and in a timely manner to any Breach of Security that does;
- (c) identify and implement changes to the Supplier System to prevent future any Breach of Security; and
- (d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

(the "**Protective Monitoring System**").

15.2 The Protective Monitoring System must provide for:

- (a) event logs and audit records of access to the Supplier System; and
- (b) regular reports and alerts to identify:
 - ix. changing access trends;
 - x. unusual usage patterns; or
 - xi. the access of greater than usual volumes of Government Data; and
 - xii. the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

16 PATCHING

16.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

(a) the Supplier must patch any vulnerabilities classified as “**critical**”:

- xiii. if it is technically feasible to do so, within 5 Working Days of the public release;
or
- xiv. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as “**important**”:

- i. if it is technically feasible to do so, within 1 month of the public release; or
- ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(b)(i), then as soon as reasonably practicable after the public release;

(c) the Supplier must remedy any vulnerabilities classified as “**other**” in the public release:

- i. if it is technically feasible to do so, within 2 months of the public release; or
- ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 17.1(c)(i), then as soon as reasonably practicable after the public release;

(d) where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

17 MALWARE PROTECTION

17.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

17.2 The Supplier must ensure that such Anti-virus Software:

- (a) prevents the installation of the most common forms of Malicious Software in the Supplier System;
- (b) performs regular scans of the Supplier System to check for Malicious Software; and
- (c) where Malicious Software has been introduced into the Supplier System, so far as practicable
 - iii. prevents the harmful effects from the Malicious Software; and
 - iv. removes the Malicious Software from the Supplier System.

18 END-USER DEVICES

18.1 The Supplier must, and must ensure that all Subcontractors, manage all End-User Devices on which Government Data is stored or Handled in accordance with the following requirements:

- (a) the operating system and any applications that store, Handle or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
- (b) users must authenticate before gaining access;
- (c) all Government Data must be encrypted using a suitable encryption tool;
- (d) the End-User Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-User Device is inactive;
- (e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

(f) the Supplier or Subcontractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

(g) all End-User Devices are within the scope of any required Certification.

18.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

19 VULNERABILITY SCANNING

19.1 The Supplier must:

- (a) scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and
- (b) if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 14.

20. ACCESS CONTROL

20.1 The Supplier must, and must ensure that all Subcontractors:

- (a) identify and authenticate all persons who access the Supplier System before they do so;
- (b) require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;
- (c) allow access only to those parts of the Supplier System and Sites that those persons require;
- (d) maintain records detailing each person's access to the Supplier System.

20.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier System:

- (a) are allocated to a single, individual user;
- (b) are accessible only from dedicated End-User Devices;
- (c) are configured so that those accounts can only be used for system administration tasks;
- (d) require passwords with high complexity that are changed regularly;
- (e) automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and
- (f) are:
 - v. restricted to a single role or small number of roles;
 - vi. time limited; and
 - vii. restrict the Privileged User's access to the internet.

21. REMOTE WORKING

21.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

- (a) unless in writing by the Authority, Privileged Users do not undertake Remote Working;
- (b) where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

21.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

- (a) prepare and have approved by the Buyer in the Remote Working Policy in accordance with this Paragraph;
- (b) undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

(c) ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

(d) may not permit any Supplier Staff or the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

21.3 The Remote Working Policy must include or make provision for the following matters:

(a) restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

(b) restricting or prohibiting Supplier Staff from downloading any Government Data to any End-User Device other than an End User Device that:

- i. is provided by the Supplier or Sub-contractor (as appropriate); and
- ii. complies with the requirements set out in Paragraph 3 (*End-User Devices*);

(c) ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

(d) giving effect to the Security Controls (so far as they are applicable); and

(e) for each different category of Supplier Staff subject to the proposed Remote Working Policy:

- i. the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;
- ii. any identified security risks arising from the proposed Handling in a Remote Location;
- iii. the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and
- iv. the business rules with which the Supplier Staff must comply.

21.4 The Supplier may submit a proposed Remote Working Policy for consideration at any time.

22 BACKUP AND RECOVERY OF GOVERNMENT DATA

22.1 The Supplier must ensure that the Supplier System:

- (a) backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and
- (b) retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

22.2 The Supplier must ensure the Supplier System:

- (a) uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;
- (b) the backup system monitors backups of Government Data to:
 - i. identify any backup failure; and
 - ii. confirm the integrity of the Government Data backed up;
- (c) any backup failure is remedied properly;
- (d) the backup system monitors backups of Government Data to:
 - i. identify any recovery failure; and
 - ii. confirm the integrity of Government Data recovered; and
- (e) any recovery failure is promptly remedied.

23 RETURN AND DELETION OF GOVERNMENT DATA

23.1 Subject to Paragraph 24.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

- (a) securely erase any or all Government Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

- (b) provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

23.2 Paragraph 24.1 does not apply to Government Data:

- (a) that is Personal Data in respect of which the Supplier is a Controller;
- (b) to which the Supplier has rights to Handle independently from this Contract; or
- (c) in respect of which, the Supplier is under an obligation imposed by Law to retain.

23.3 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor:

- (a) when requested to do so by the Buyer; and
- (b) using the method specified by the Buyer.

24 PHYSICAL SECURITY

24.2 The Supplier must, and must ensure that Subcontractors, store the Government Data on servers housed in physically secure locations.

25 BREACH OF SECURITY

25.2 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

- (a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;
- (b) provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction;
- (c) where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.