SHORT FORM CONTRACT FOR THE SUPPLY OF SERVICES

I. Index

III.Cover Letter

Opus 2 International Limited

5 New Street Square,

London,

EC4A 3BF

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

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

Date: 19 December 2023

Our ref: GTIS19A39

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

Following your proposal for the supply of Specialist Electronic Hearing Management for the Cabinet Office, we are pleased to confirm our intention to award this Contract to you.

The attached Order Form, contract Conditions and the Annexes set out the terms of the Contract between Cabinet Office and Opus International Ltd for the provision of the Deliverables set out in the Order Form.

We thank you for your cooperation to date, and look forward to forging a successful working relationship resulting in a smooth and successful Delivery of the Deliverables. Please confirm your acceptance of this Contract by signing and returning the Order Form to **REDACTED TEXT under FOIA Section 40, Personal Information** at the following email address: **REDACTED TEXT under FOIA Section 40, Personal Information** within 7 days from the date of the Order Form. No other form of acknowledgement will be accepted. Please remember to include the reference number above in any future communications relating to this Contract.

We will then arrange for the Order Form to be countersigned which will create a binding contract between us.

Yours faithfully,

REDACTED TEXT under FOIA Section 40, Personal Information

IV.Order Form

1. **Contract Reference**	GTIS19A39	
2. **Buyer**	Grenfell Tower Inquiry of 1 Giltspur Street, London, EC1A 9DD. 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**	Opus 2 International Limited 5 New Street Square, London, EC4A 3BF **Company Number:** 05907841	
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 and Annexes. Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in the Conditions.	
5. **Deliverables**	**Goods**	None
	Services	The services will be delivered as a cloud-based legal and technological service to the Buyer as further described in **Annex 2.**

6. **Specification**	The specification of the Deliverables is as set out in **Annex 2** .
7. **Start Date**	01 January 2024
8. **Expiry Date**	30 June 2024
9. **Extension Period**	Subject to further budgetary approval, the Buyer may extend the Contract for a period of up to 6 Months, subject to necessary internal budgetary and commercial approvals, 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**	N/A
11. **Optional Intellectual**	N/A

Property Rights ("IPR") Clauses	
12. **Charges**	The Charges for the Deliverables under this Contract are set out in **Annex 3** and are as follows: £130,000 excluding VAT Value may be higher where extension periods are exercised or changes to services provided are made, this will be subject to additional budgetary and commercial approval. In line with G-Cloud, all fees and rates agreed in the previous Call-Off Contract (CCTS19A38) shall apply.

13. **Payment**	Payment of undisputed invoices will be made within 30 days of receipt of invoice, which must be submitted promptly by the Supplier. All invoices must be sent, quoting a valid Purchase Order Number (PO Number) and any other relevant details, to: apinvoices-cab-u@gov.sscl.com copying in finance@grenfelltowerinquiry.org.uk and **REDACTED TEXT under FOIA Section 40, Personal Information** 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. 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. Payments will be made by BACS Payment Method. If you have a query regarding an outstanding payment please contact our Finance team either by email to: finance@grenfelltowerinquiry.org.uk between 09:00-17:00 Monday to Friday.
14. **Data Protection Liability Cap**	In accordance with clause 12.6 of the Conditions, the Supplier's total aggregate liability under clause 14.7.5 of the Conditions is in line with the Data Protection Liability Cap, being £5 million.
15. **Buyer Authorised**	For general liaison your contact will continue to be **REDACTED TEXT under FOIA Section 40, Personal Information**

Representative (s)	or, in their absence, **REDACTED TEXT under FOIA Section 40, Personal Information**
16. **Supplier Authorised Representative (s)**	**REDACTED TEXT under FOIA Section 40, Personal Information** **REDACTED TEXT under FOIA Section 40, Personal Information**

17. **Address for notices**	Grenfell Tower Inquiry 1 Giltspur Street, London, EC1A 9DD Attention: **REDACTED TEXT under FOIA Section 40, Personal Information** Email: **REDACTED TEXT under FOIA Section 40, Personal Information**	Opus 2 International Limited 5 New Street Square, London, EC4A 3BF Attention: **REDACTED TEXT under FOIA Section 40, Personal Information** Email **REDACTED TEXT under FOIA Section 40, Personal Information**
18. **Key Staff**	**REDACTED TEXT under FOIA Section 40, Personal Information**	
19. **Procedures and Policies**	For the purposes of the Contract the: Cabinet Office's Staff Vetting Procedures are: The Buyer requires the Supplier to ensure that any person employed in the Delivery of the Deliverables has undertaken a Disclosure and Barring Service (DBS) check. For the purposes of clause 8.7 of the Conditions: Relevant convictions 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), driving offences, offences against property, drugs, alcohol, public order offences or any other offences relevant to Services as the Buyer may specify.	

	Cabinet Office's additional sustainability requirement can be found in the following link: https://www.gov.uk/government/publications/sustainability-in-ukhsa/environmental-polic y Cabinet Office's equality and diversity policy can be found at: https://www.gov.uk/government/organisations/cabinet-office/about/equality-and-diversit y
20. **Special Terms**	N/A
21. **Incorporated Terms**	The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies: (a) The cover letter from the Buyer to the Supplier dated 19 December 2023 (b) This Order Form (c) Any Special Terms (see row 21 (Special Terms) in this Order Form) (d) Conditions (e) The following Annexes in equal order of precedence: i. Annex 1 – Processing Personal Data ii. Annex 2 – Specification iii. Annex 3 – Charges iv. Annex 6 - Security Management

Signed for and on behalf of the Supplier	Signed for and on behalf of the Buyer acting on behalf of the Crown
Name: **REDACTED TEXT under FOIA Section 40, Personal Information**	Name: **REDACTED TEXT under FOIA Section 40, Personal Information**
Date: 22/12/23	Date: 22 December 2023
Signature: **REDACTED TEXT under FOIA Section 40, Personal Information**	Signature: **REDACTED TEXT under FOIA Section 40, Personal Information**

V. 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"	the Buyer's right to: (a) verify the accuracy of the Charges and any other amounts payable by the Buyer under the Contract (including proposed or actual variations to them in accordance with the Contract); (b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Deliverables; (c) verify the Supplier's and each Subcontractor's compliance with the applicable Law; (d) identify or investigate actual or suspected breach of clauses 4 to 34 (inclusive), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Buyer shall have no obligation to inform the Supplier of the purpose or objective of its investigations; (e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any Subcontractors or their ability to provide the Deliverables; (f) obtain such information as is necessary to fulfil the Buyer's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; (g) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Contract; (h) carry out the Buyer's internal and statutory audits and to prepare, examine and/or certify the Buyer's annual and interim reports and accounts; (i) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Buyer has used its resources;

"Beneficiary"	A Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer Cause"	has the meaning given to it in the Order Form;
"Buyer"	the person named as Buyer in the Order Form. Where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole;

"Charges"	the charges for the Deliverables as specified in the Order Form;
"Claim"	any claim which it appears that the Buyer is, or may become, entitled to indemnification under this Contract;
"Conditions"	means these short form terms and conditions of contract;
"Confidential Information"	all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (a) is known by the receiving Party to be confidential; (b) is marked as or stated to be confidential; or (c) ought reasonably to be considered by the receiving Party to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Contract, in the reasonable opinion of the Buyer;
"Contract"	the contract between the Buyer and the Supplier which is created by the Supplier's counter signing the Order Form and includes the cover letter (if used), Order Form, these Conditions and the Annexes;
"Controller"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the Welsh Government), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;

"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Legislation"	(a) the UK GDPR, (b) the DPA 2018; (c) all applicable Law about the processing of personal data and privacy and guidance issued by the Information Commissioner and other regulatory authority; and (d) (to the extent that it applies) the EU GDPR (and in the event of conflict, the UK GDPR shall apply);
"Data Protection Liability Cap"	has the meaning given to it in row 14 of the Order Form;
"Data Protection Officer"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Data Subject"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Deliver"	hand over of the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and stacking and any other specific arrangements agreed in accordance with clause 4.2. "Delivered" and "Delivery" shall be construed accordingly;
"Deliverables"	means the Goods, Services, and/or software to be supplied under the Contract as set out in the Order Form;
"DPA 2018"	the Data Protection Act 2018;

"EU GDPR"	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
"Existing IPR"	any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise);
"Expiry Date"	the date for expiry of the Contract as set out in the Order Form;

"FOIA"	the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;

"Force Majeure Event"	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 delay the Affected Party from performing its obligations under the Contract; (b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; (c) acts of a Crown Body, local government or regulatory bodies; (d) fire, flood or any disaster; or (e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: (a) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; (b) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and (c) any failure of delay caused by a lack of funds, and which is not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party;
"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"	(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: (i) are supplied to the Supplier by or on behalf of the Buyer; or

	(ii) the Supplier is required to generate, process, store or transmit pursuant to the Contract; or (b) any Personal Data for which the Buyer is the Controller;
"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"	in respect of a person: (a) if that person is insolvent; (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); (c) if an administrator or administrative receiver is appointed in respect of the whole or any part of the person's assets or business; (d) if the person makes any composition with its creditors; or (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;
"IP Completion Day"	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;
"Joint Controller Agreement"	the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Part B Joint Controller Agreement *(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-standa rds-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: (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;
"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"	the Supplier's plan (or revised plan) to rectify its Material Breach which shall include: (a) full details of the Material Breach that has occurred, including a root cause analysis; (b) the actual or anticipated effect of the Material Breach; and (c) the steps which the Supplier proposes to take to rectify the Material Breach (if applicable) and to prevent such Material Breach from recurring, including timescales for such steps and for the rectification of the Material Breach (where applicable);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time;
"Request For Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "**request**" shall apply);
"Services"	the services to be supplied by the Supplier to the Buyer under the Contract;
"Specification"	the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form;
"Staff Vetting Procedures"	vetting procedures that accord with Good Industry Practice or, where applicable, the Buyer's procedures or policies for the vetting of personnel as specified in the Order Form or provided to the Supplier in writing following agreement to the same by the Supplier from time to time;
"Start Date"	the start date of the Contract set out in the Order Form;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party: (a) provides the Deliverables (or any part of them); (b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or (c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);

"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third party appointed to process Personal Data on behalf of the Processor related to the Contract;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier's obligations under the Contract;
"Supplier"	the person named as Supplier in the Order Form;
"Term"	the period from the Start Date to the Expiry Date as such period may be extended in accordance with clause 11.2 or terminated in accordance with the Contract;
"Third Party IPR"	intellectual property rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Transparency Information"	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-updateto-transparency-principles) as updated from time to time except for: (a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Buyer; and (b) Confidential Information;
"UK GDPR"	has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;

"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policynote-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 and the Contract;

4.1.1.2 using reasonable skill and care;

4.1.1.3 using Good Industry Practice;

4.1.1.4 using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract; 4.1.1.5 on the dates agreed; and

4.1.1.6 that comply with all Law.

4.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days (or longer where the Supplier offers a longer warranty period to its Buyers) from Delivery against all obvious defects.

4.2 Goods clauses

4.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

4.2.2 The Supplier transfers ownership of the Goods on completion of Delivery or payment for those Goods, whichever is earlier.

4.2.3 Risk in the Goods transfers to the Buyer on Delivery, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

4.2.4 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

4.2.5 The Supplier must Deliver the Goods on the date and to the location specified in the Order Form, during the Buyer's working hours (unless otherwise specified in the Order Form).

4.2.6 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

4.2.7 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

4.2.8 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

4.2.9 The Supplier will notify the Buyer of any request that Goods are returned to it or the manufacturer after the discovery of safety issues or defects that might endanger health or hinder performance and shall indemnify the Buyer against the costs arising as a result of any such request.

4.2.10 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable endeavours to minimise these costs.

4.2.11 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with clause 4.2. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

4.2.12 The Buyer will not be liable for any actions, claims, costs and expenses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Buyer or its servant or agent. If the Buyer suffers or incurs any damage or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Buyer from any losses, charges, costs or expenses which arise as a result of or in connection with such damage or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Staff.

4.3 **Services clauses**

4.3.1 Late Delivery of the Services will be a default of the Contract.

4.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions including the security requirements (where any such requirements have been provided).

4.3.3 The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services

4.3.4 The Supplier must at its own risk and expense provide all equipment required to deliver the Services. Any equipment provided by the Buyer to the Supplier for supplying the Services remains the property of the Buyer and is to be returned to the Buyer on expiry or termination of the Contract.

4.3.5 The Supplier must allocate sufficient resources and appropriate expertise to the Contract.

4.3.6 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

4.3.7 On completion of the Services, the Supplier is responsible for leaving the Buyer's premises in a clean, safe and tidy condition and making good any damage that it has caused to the Buyer's premises or property, other than fair wear and tear.

4.3.8 The Supplier must ensure all Services, and anything used to deliver the Services, are of good quality and free from defects.

4.3.9 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

5 PRICING AND PAYMENTS

5.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the charges in the Order Form.

5.2 All Charges:

5.2.1 exclude VAT, which is payable on provision of a valid VAT invoice; and

5.2.2 include all costs and expenses connected with the supply of Deliverables.

5.3 The Buyer must pay the Supplier the charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds to the Supplier's account stated in the invoice or in the Order Form.

5.4 A Supplier invoice is only valid if it:

5.4.1 includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer; and

5.4.2 includes a detailed breakdown of Deliverables which have been delivered.

5.5 If there is a dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 36.

5.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier under this Contract or any other agreement between the Supplier and the Buyer if notice and reasons are provided.

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

6 THE BUYER'S OBLIGATIONS TO THE SUPPLIER

6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:

6.1.1 the Buyer cannot terminate the Contract under clause 11;

6.1.2 the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;

6.1.3 the Supplier is entitled to additional time needed to deliver the Deliverables; and

6.1.4 the Supplier cannot suspend the ongoing supply of Deliverables.

6.2 Clause 6.1 only applies if the Supplier:

6.2.1 gives notice to the Buyer within 10 Working Days of becoming aware; 6.2.2

demonstrates that the failure only happened because of the Buyer Cause; and

6.2.3 mitigated the impact of the Buyer Cause.

7 RECORD KEEPING AND REPORTING

7.1 The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in the Order Form.

7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the date of expiry or termination of the Contract and in accordance with the UK GDPR or the EU GDPR as the context requires.

7.3 The Supplier must allow any auditor appointed by the Buyer access to its premises to verify all contract accounts and records of everything to do with the Contract and provide copies for the Audit.

7.4 The Buyer or an auditor can Audit the Supplier.

7.5 During an Audit, the Supplier must provide information to the auditor and reasonable co-operation at their request.

7.6 The Parties will bear their own costs when an Audit is undertaken unless the Audit identifies a Material Breach by the Supplier, in which case the Supplier will repay the Buyer's reasonable costs in connection with the Audit.

7.7 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

7.7.1 tell the Buyer and give reasons;

7.7.2 propose corrective action; and

7.7.3 provide a deadline for completing the corrective action.

7.8 If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Contract then the Buyer may:

7.8.1 require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand; and

7.8.2 if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Contract immediately for Material Breach (or on such date as the Buyer notifies) and the consequences of termination in Clause 11.5.1 shall apply.

7.9 If there is a Material Breach, the Supplier must notify the Buyer within 3 Working Days of the Supplier becoming aware of the Material Breach. The Buyer may request that the Supplier provide a Rectification Plan within 10 Working Days of the Buyer's request alongside any additional documentation that the Buyer requires. Once such Rectification Plan is agreed between the Parties (without the Buyer limiting its rights) the Supplier must immediately start work on the actions in the Rectification Plan at its own cost.

8 SUPPLIER STAFF

8.1 The Supplier Staff involved in the performance of the Contract must:

8.1.1 be appropriately trained and qualified;

8.1.2 be vetted in accordance with the Staff Vetting Procedures; and

8.1.3 comply with all conduct requirements when on the Buyer's premises.

8.2 Where the Buyer decides one of the Supplier's Staff isn't suitable to work on the Contract, the Supplier must replace them with a suitably qualified alternative.

8.3 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.

8.4 The Supplier indemnifies the Buyer against all claims brought by any person employed or engaged by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8.5 The Buyer indemnifies the Supplier against all claims brought by any person employed or engaged by the Buyer caused by an act or omission of the Buyer or any of the Buyer's employees, agents, consultants and contractors.

8.6 The Supplier shall use those persons nominated (if any) as Key Staff in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier to provide the Deliverables and shall not remove or replace any of them unless:

8.6.1 requested to do so by the Buyer or the Buyer approves such removal or replacement (not to be unreasonably withheld or delayed);

8.6.2 the person concerned resigns, retires or dies or is on parental or long-term sick leave; or

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

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

9 RIGHTS AND PROTECTION

9.1 The Supplier warrants and represents that:

9.1.1 it has full capacity and authority to enter into and to perform the Contract;

9.1.2 the Contract is entered into by its authorised representative;

9.1.3 it is a legally valid and existing organisation incorporated in the place it was formed;

9.1.4 there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;

9.1.5 all necessary rights, authorisations, licences and consents (including in relation to IPRs) are in place to enable the Supplier to perform its obligations under the Contract and the Buyer to receive the Deliverables;

9.1.6 it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and

9.1.7 it is not impacted by an Insolvency Event.

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

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

9.3.1 wilful misconduct of the Supplier, any of its Subcontractor and/or Supplier Staff that impacts the Contract; and

9.3.2 non-payment by the Supplier of any tax or National Insurance.

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

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

10 INTELLECTUAL PROPERTY RIGHTS ("IPRS")

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

10.1.1 receive and use the Deliverables; and

10.1.2 use the New IPR.

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

10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a royalty-free, non-exclusive, non-transferable licence to use, copy, and adapt any Existing IPRs and the New IPR which the Supplier reasonably requires for the purpose of fulfilling its obligations during the Term and commercially exploiting the New IPR developed under the Contract. This licence is sub-licensable to a Subcontractor for the purpose of enabling the Supplier to fulfil its obligations under the Contract, and in that case the Subcontractor must enter into a confidentiality undertaking with the Supplier on the same terms as set out in clause 15 (What you must keep confidential).

10.3 Unless otherwise agreed in writing, the Supplier and the Buyer will record any New IPR and keep this record updated throughout the Term.

10.4 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract, it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

10.5 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in this clause 10 or otherwise agreed in writing.

10.6 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

10.7 If an IPR Claim is made or anticipated, the Supplier must at its own option and expense, either:

10.7.1 obtain for the Buyer the rights in clause 10.1 without infringing any third party intellectual property rights; and

10.7.2 replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

10.7.3 If the Supplier is not able to resolve the IPR Claim to the Buyer's reasonable satisfaction within a reasonable time, the Buyer may give written notice that it terminates the Contract from the date set out in the notice, or where no date is given in the notice, the date of the notice. On termination, the consequences of termination in clauses 11.5.1 shall apply.

10.8 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless:

10.8.1 the Buyer gives its approval to do so; and

10.8.2 one of the following conditions applies:

10.8.2.1 the owner or an authorised licensor of the relevant Third Party IPR has granted the Buyer a direct licence that provides the Buyer with the rights in clause 10.1; or

10.8.2.2 if the Supplier cannot, after commercially reasonable endeavours, obtain for the Buyer a direct licence to the Third Party IPR as set out in clause 10.8.2.1:

(a) the Supplier provides the Buyer with details of the licence terms it can obtain and the identity of those licensors;

(b) the Buyer agrees to those licence terms; and

(c) the owner or authorised licensor of the Third Party IPR grants a direct licence to the Buyer on those terms; or

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

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

11 ENDING THE CONTRACT

11.1 The Contract takes effect on the Start Date and ends on the earlier of the Expiry Date or termination of the Contract, or earlier if required by Law.

11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form.

11.3 **Ending the Contract without a reason**

11.3.1 The Buyer has the right to terminate the Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice, and if it's terminated clause 11.6.2 applies.

11.4 **When the Buyer can end the Contract**

11.4.1 If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier and the consequences of termination in Clause 11.5.1 shall apply:

11.4.1.1 there's a Supplier Insolvency Event;

11.4.1.2 the Supplier is in Material Breach of the Contract;

11.4.1.3 there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which isn't pre-approved by the Buyer in writing;

11.4.1.4 the Buyer discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded;

11.4.1.5 the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them; or

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

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

11.5 **What happens if the Contract ends**

11.5.1 Where the Buyer terminates the Contract under clause 10.9, 11.4, 7.8.2, 28.4.2, or Paragraph 8 of Part B Joint Controller Agreement *(Optional)* of Annex 1 – Processing Personal Data (if used), all of the following apply:

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

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

11.5.1.3 accumulated rights of the Parties are not affected;

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

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

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

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

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

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

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

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

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

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

11.6.2.3 clauses 11.5.1.2 to 11.5.1.7 apply.

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

11.7 **Partially ending and suspending the Contract**

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

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

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

11.7.3.1 reject the variation; or

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

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

12 HOW MUCH YOU CAN BE HELD RESPONSIBLE FOR

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

12.2 No Party is liable to the other for:

12.2.1 any indirect losses; and/or

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

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

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

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

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

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

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

12.6 Notwithstanding clause 12.1, but subject to clauses 12.1 and 12.3, the Supplier's total aggregate liability under clause 14.7.5 shall not exceed the Data Protection Liability Cap.

12.7 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.

12.8 If more than one Supplier is party to the Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

13 OBEYING THE LAW

13.1 The Supplier, in connection with provision of the Deliverables:

13.1.1 is expected to meet and have its Subcontractors meet the standards set out in the Supplier Code of Conduct: (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1163536/Supplier_Code_of_Conduct_v3.pdff) 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),[1] as such clauses may be amended or updated from time to time; and

13.1.5 meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs, as updated from time to time.

13.2 The Supplier indemnifies the Buyer against any costs resulting from any default by the Supplier relating to any applicable Law to do with the Contract.

13.3 The Supplier must appoint a compliance officer who must be responsible for ensuring that the Supplier complies with Law, clause 13.1 and clauses 27 to 34.

14 Data Protection and Security

14.1 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.2 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies via secure encrypted method upon reasonable request.

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

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

14.5.2 restore the Government Data itself or using a third party.

14.6 The Supplier must pay each Party's reasonable costs of complying with clause 14.5 unless the Buyer is at fault.

14.7 The Supplier:

14.7.1 must provide the Buyer with all Government Data in an agreed format (provided it is secure and readable) within 10 Working Days of a written request;

14.7.2 must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;

14.7.3 must securely destroy all storage media that has held Government Data at the end of life of that media using Good Industry Practice, other than in relation to Government Data which is owned or licenced by the Supplier or in respect of which the Parties are Independent Controllers or Joint Controllers;

14.7.4 securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it, other than in relation to Government Data which is owned or licenced by the Supplier or in respect of which the Parties are Independent Controllers or Joint Controllers; and

14.7.5 indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation.

14.8 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Contract dictates the status of each party under the DPA 2018. A Party may act as:

14.8.1 “Controller” in respect of the other Party who is “Processor”;

14.8.2 “Processor” in respect of the other Party who is “Controller”;

14.8.3 “Joint Controller” with the other Party;

14.8.4 “Independent Controller” of the Personal Data where the other Party is also “Controller”,

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

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

14.9.1 Where a Party is a Processor, the only processing that the Processor is authorised to do is listed in Part A Authorised Processing Template of Annex 1 – Processing Personal Data by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).

14.9.2 The Processor must notify the Controller immediately if it thinks the Controller's instructions breach the Data Protection Legislation.

14.9.3 The Processor must give all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment before starting any processing, which may include, at the discretion of the Controller:

14.9.3.1 a systematic description of the expected processing and its purpose;

14.9.3.2 the necessity and proportionality of the processing operations;

14.9.3.3 the risks to the rights and freedoms of Data Subjects; and

14.9.3.4 the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.

14.9.4 The Processor must, in in relation to any Personal Data processed under this Contract:

14.9.4.1 process that Personal Data only in accordance with Part A Authorised Processing Template of Annex 1 – Processing Personal Data unless the Processor is required to do otherwise by Law. If lawful to notify the Controller, the Processor must promptly notify the Controller if the Processor is otherwise required to process Personal Data by Law before processing it.

14.9.4.2 put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Controller.

14.9.4.3 Ensure that:

(a) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Part A Authorised Processing Template of Annex 1 – Processing Personal Data);

(b) it uses best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Processor's duties under this clause 14;

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(iii) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise allowed by the Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data.

(c) the Processor must not transfer Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(d) the transfer is in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018) and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or

(e) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or the transfer is in accordance with Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:

(i) where the transfer is subject to UK GDPR:

(A) the International Data Transfer Agreement (the "**IDTA**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018 as well as any additional measures determined by the Controller;

(B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time ("**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or (ii)

where the transfer is subject to EU GDPR, the EU SCCs,

as well as any additional measures determined by the

Controller being implemented by the importing party;

(f) the Data Subject has enforceable rights and effective legal remedies when transferred;

(g) the Processor meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

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

14.9.5 The Processor must at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data. 14.9.6 The Processor must notify the Controller immediately if it:

14.9.6.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

14.9.6.2 receives a request to rectify, block or erase any Personal Data;

14.9.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

14.9.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;

14.9.6.5 receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; and

14.9.6.6 becomes aware of a Data Loss Event.

14.9.7 Any requirement to notify under clause 14.9.6 includes the provision of further information to the Controller in stages as details become available.

14.9.8 The Processor must promptly provide the Controller with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.9.6. This includes giving the Controller:

14.9.8.1 full details and copies of the complaint, communication or request;

14.9.8.2 reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;

14.9.8.3 any Personal Data it holds in relation to a Data Subject on request;

14.9.8.4 assistance that it requests following any Data Loss Event; and

14.9.8.5 assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office or any other regulatory authority.

14.9.9 The Processor must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Processor employs fewer than 250 staff, unless either the Controller determines that the processing:

14.9.9.1 is not occasional;

14.9.9.2 includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

14.9.9.3 is likely to result in a risk to the rights and freedoms of Data Subjects.

14.9.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

14.9.11 Before allowing any Subprocessor to process any Personal Data, the Processor must:

14.9.11.1 notify the Controller in writing of the intended Subprocessor and processing;

14.9.11.2 obtain the written consent of the Controller;

14.9.11.3 enter into a written contract with the Subprocessor so that this clause 14 applies to the Subprocessor; and

14.9.11.4 provide the Controller with any information about the Subprocessor that the Controller reasonably requires.

14.9.12 The Processor remains fully liable for all acts or omissions of any Subprocessor.

14.9.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other regulatory authority.

14.10 **Joint Controllers of Personal Data**

14.10.1 In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Part B Joint Controller Agreement *(Optional)* of Annex 1 – Processing Personal Data.

14.11 **Independent Controllers of Personal Data**

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

15 WHAT YOU MUST KEEP CONFIDENTIAL

15.1 Each Party must:

15.1.1 keep all Confidential Information it receives confidential and secure;

15.1.2 not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract; and

15.1.3 immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:

15.2.1 where disclosure is required by applicable Law if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;

15.2.2 if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;

15.2.3 if the information was given to it by a third party without obligation of confidentiality;

15.2.4 if the information was in the public domain at the time of the disclosure;

15.2.5 if the information was independently developed without access to the disclosing Party's Confidential Information;

15.2.6 on a confidential basis, to its auditors or for the purposes of regulatory requirements;

15.2.7 on a confidential basis, to its professional advisers on a need-to-know basis; and

15.2.8 to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.

15.4 The Buyer may disclose Confidential Information in any of the following cases:

15.4.1 on a confidential basis to the employees, agents, consultants and contractors of the Buyer;

15.4.2 on a confidential basis to any Crown Body, any successor body to a Crown Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;

15.4.3 if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;

15.4.4 where requested by Parliament; and

15.4.5 under clauses 5.7 and 16.

15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.

15.6 Transparency Information, and Information which is exempt from disclosure by clause 16 is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable endeavours to ensure that Supplier Staff do not either.

16 When you can share information

16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.

16.2 In accordance with a reasonable timetable and in any event within 5 Working Days of a request from the Buyer, the Supplier must give the Buyer full co-operation and information needed so the Buyer can:

16.2.1 comply with any Request For Information

16.2.2 if the Contract has a value over the relevant threshold in Part 2 of the Regulations, comply with any of its obligations in relation to publishing Transparency Information.

16.3 To the extent that it is allowed and practical to do so, the Buyer will use reasonable endeavours to notify the Supplier of a Request For Information and may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure is the Buyer's decision in its absolute discretion.

17 Insurance

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

18 Invalid parts of the contract

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

19 Other people's rights in the contract

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

20 Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Contract while the inability to perform continues, if it both:

20.1.1 provides written notice to the other Party; and

20.1.2 uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Any failure or delay by the Supplier to perform its obligations under the Contract that is due to a failure or delay by an agent, Subcontractor and/or Supplier Staff will only be considered a Force Majeure Event if that third party is itself prevented from complying with an obligation to the Supplier due to a Force Majeure Event.

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

20.4 Where a Party terminates under clause 20.3:

20.4.1 each Party must cover its own losses; and

20.4.2 clauses 11.5.1.2 to 11.5.1.7 apply.

21 RELATIONSHIPS CREATED BY THE CONTRACT

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

22 GIVING UP CONTRACT RIGHTS

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

23 TRANSFERRING RESPONSIBILITIES

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

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

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

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

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

24 SUPPLY CHAIN

24.1 The Supplier cannot sub-contract the Contract or any part of it without the Buyer's prior written consent. The Supplier shall provide the Buyer with the name of any Subcontractor the Supplier

proposes to engage for the purposes of the Contract. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. If the Buyer does not communicate a decision to the Supplier within 10 Working Days of the request for consent then its consent will be deemed to have been given. The Buyer may reasonably withhold its consent to the appointment of a Subcontractor if it considers that:

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

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

24.1.3 the proposed Subcontractor employs unfit persons.

24.2 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of all such Subcontractors at all levels of the supply chain including:

24.2.1 their name;

24.2.2 the scope of their appointment; and

24.2.3 the duration of their appointment.

24.3 The Supplier must exercise due skill and care when it selects and appoints Subcontractors.

24.4 For Sub-Contracts in the Supplier's supply chain entered into wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract:

24.4.1 where such Sub-Contracts are entered into after the Start Date, the Supplier will ensure that they all contain provisions that; or

24.4.2 where such Sub-Contracts are entered into before the Start Date, the Supplier will take all reasonable endeavours to ensure that they all contain provisions that:

24.4.2.1 allow the Supplier to terminate the Sub-Contract if the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law;

24.4.2.2 require the Supplier to pay all Subcontractors in full, within 30 days of receiving a valid, undisputed invoice; and

24.4.2.3 allow the Buyer to publish the details of the late payment or non-payment if this 30-day limit is exceeded.

24.5 At the Buyer's request, the Supplier must terminate any Sub-Contracts in any of the following events:

24.5.1 there is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 of a Subcontractor which isn't pre-approved by the Buyer in writing;

24.5.2 the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 11.4;

24.5.3 a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Buyer;

24.5.4 the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law; and/or

24.5.5 the Buyer has found grounds to exclude the Subcontractor in accordance with Regulation 57 of the Regulations.

24.6 The Supplier is responsible for all acts and omissions of its Subcontractors and those employed or engaged by them as if they were its own.

25 CHANGING THE CONTRACT

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

26 HOW TO COMMUNICATE ABOUT THE CONTRACT

26.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9am on the first Working Day after sending unless an error message is received.

26.2 Notices to the Buyer or Supplier must be sent to their address or email address in the Order Form.

26.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

27 DEALING WITH CLAIMS

27.1 If a Beneficiary becomes aware of any Claim, then it must notify the Indemnifier as soon as reasonably practical.

27.2 at the Indemnifier's cost the Beneficiary must:

27.2.1 allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim;

27.2.2 give the Indemnifier reasonable assistance with the Claim if requested; and

27.2.3 not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

27.3 The Beneficiary must:

27.3.1 consider and defend the Claim diligently and in a way that does not damage the Beneficiary's reputation; and

27.3.2 not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

28 PREVENTING FRAUD, BRIBERY AND CORRUPTION

28.1 The Supplier shall not:

28.1.1 commit any criminal offence referred to in 57(1) and 57(2) of the Regulations; or

28.1.2 offer, give, or agree to give anything, to any person (whether working for or engaged by the Buyer or any other public body) an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Contract or any other public function or for showing or refraining from showing favour or disfavour to any person in relation to the Contract or any other public function.

28.2 The Supplier shall take all reasonable endeavours (including creating, maintaining and enforcing adequate policies, procedures and records), in accordance with Good Industry Practice, to prevent any matters referred to in clause 28.1 and any fraud by the Supplier Staff and the Supplier (including its shareholders, members and directors) in connection with the Contract and shall notify the Buyer immediately if it has reason to suspect that any such matters have occurred or is occurring or is likely to occur.

28.3 If the Supplier notifies the Buyer as required by clause 28.2, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

28.4 If the Supplier or the Supplier Staff engages in conduct prohibited by clause 28.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Buyer) the Buyer may:

28.4.1 require the Supplier to remove any Supplier Staff from providing the Deliverables if their acts or omissions have caused the default; and

28.4.2 immediately terminate the Contract and the consequences of termination in Clause 11.5.1 shall apply.

29 EQUALITY, DIVERSITY AND HUMAN RIGHTS

29.1 The Supplier must follow all applicable employment and equality Law when they perform their obligations under the Contract, including:

29.1.1 protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and

29.1.2 any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

29.2 The Supplier must use all reasonable endeavours, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

30 HEALTH AND SAFETY

30.1 The Supplier must perform its obligations meeting the requirements of:

30.1.1 all applicable Law regarding health and safety; and

30.1.2 the Buyer's current health and safety policy while at the Buyer's premises, as provided to the Supplier.

30.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer premises that relate to the performance of the Contract.

31 ENVIRONMENT AND SUSTAINABILITY

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

31.1.1 meet, in all material respects, the requirements of all applicable Laws regarding the environment; and

31.1.2 comply with its obligations under the Buyer's current environmental policy, which the Buyer must provide, and make Supplier Staff aware of such policy.

32 TAX

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

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

32.2.1 comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and

32.2.2 indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

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

32.3.1 the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 32.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;

32.3.2 the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;

32.3.3 the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with clause 32.2 or confirms that the Worker is not complying with those requirements; and

32.3.4 the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

33 CONFLICT OF INTEREST

33.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual, potential or perceived Conflict of Interest.

33.2 The Supplier must promptly notify and provide details to the Buyer if an actual, potential or perceived Conflict of Interest happens or is expected to happen.

33.3 The Buyer will consider whether there are any appropriate measures that can be put in place to remedy an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Buyer, such measures do not or will not resolve an actual or potential conflict of interest, the Buyer may terminate the Contract immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest and Clauses 11.5.1.2 to 11.5.1.7 shall apply.

34 REPORTING A BREACH OF THE CONTRACT

34.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of Law, clause 13.1, or clauses 27 to 33.

34.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 34.1 to the Buyer or a Prescribed Person.

35 FURTHER ASSURANCES

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

36 **RESOLVING DISPUTES**

36.1 If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute by commercial negotiation.

36.2 If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("**CEDR**") Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 36.3 to 36.5.

36.3 Unless the Buyer refers the dispute to arbitration using clause 36.4, the Parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction. :

36.4 The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

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

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

37 **WHICH LAW APPLIES**

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

VI.Annex 1 – Processing Personal Data

Part A **Authorised Processing Template**

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

The contact details of the Controller's Data Protection Officer are: **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 for each category of Personal Data	The Buyer is Controller and the Supplier is Processor
Subject matter of the processing	The principal purposes for which the Inquiry collects and processes subject matter, including personal data are: 1. the effective conduct of the public inquiry into the events surrounding the Grenfell Tower fire on 13 June 2017, and; 2. to discharge the Inquiry's duties pursuant to the legal obligations stipulated in the Inquiries Act 2005. This will typically include processing the personal data of: ● Core participants in the Inquiry, within the meaning of the Inquiries Act 2005. ● Other witnesses providing evidence to the Inquiry who are not core participants within the meaning of the Inquiries Act 2005, including Expert Witnesses appointed by the Inquiry; and members of the public.
Duration of the processing	Personal data will be processed by the Inquiry until the conclusion of the Inquiry. The exact duration is to be determined but is expected to be until at least the middle of 2023. Upon completion of the Inquiry there will be a process of archiving in accordance with the Public Records Act 1958.

Nature and purposes of the processing	The Grenfell Tower Inquiry is a public inquiry established under the Inquiries Act 2005. It is investigating the matters set out in its Terms of Reference by means of a legal process within the framework of the Inquiries Act 2005 and the Inquiry Rules 2006. In order to discharge its duties pursuant to the Inquiries Act 2005 and for the effective conduct of the Inquiry into the events surrounding the Grenfell Tower fire of 14 June 2017 the Inquiry must collect and process personal data for the purposes of its investigations and to enable it to carry out its work. The nature of the processing envisaged under the specific service consideration is: 1. to provide (host) an electronic platform for the storing, reviewing, analysing and the disclosure of documents and information containing personal data provided to the Inquiry, in line with its processes for handling personal information. These services include court reporting and electronic presentation of evidence. The personal data being processed will primarily be that which has been submitted to the Inquiry following a request from relevant individuals or organisations (through a 'Rule 9 ' letter) or data submitted voluntarily, for example a witness statement. This processing will include as a result of the actions and directions of the Buyer, its users and third parties, *inter alia* the collection, recording, organisation, structuring, storing, adaptation, alteration, retrieval, consultation, use, disclosure by transmission. electronic dissemination, alignment and/or combination and restriction of personal data. All personal information received by the Inquiry is handled fairly and lawfully in accordance with data protection legislation. The purposes for processing of data by the Inquiry include: 1. to gather evidence as part of the Inquiry's investigation; 2. to facilitate access to the Inquiry; 3. to enable witnesses to give evidence; and 4. to communicate with stakeholders and keep the public updated on the progress of the Inquiry. Personal information may also be used by the Inquiry to comply with the law and with contracts that the Inquiry has entered into. The lawful basis for the processing by the Inquiry of this information is set out in the Inquiry's Privacy Notice. This basis principally comprises statutory obligations under Article 6(1)(e) of the General Data

	Protection Regulation (GDPR) - '*processing that is necessary for the performance of a task carried out in the public interest or in the exercise*

	*of official authority vested in the controlle*r' - and Article 6 (1)(c) GDPR - 'processing necessary for compliance with a legal obligation.' The Supplier is reliant on this lawful basis in ensuring that the buyer is compliant with applicable laws but itself relies on its legitimate interests in providing the requested Services to the Buyer, its users and third parties.
Type of Personal Data being processed	The following is a non-exhaustive list of categories of personal data that will be processed: Personal data - this is typically biographical data such as: ● Name ● Date of Birth ● Personal Description ● Contact details, such as email addresses and telephone numbers, still images, voice and video recordings, which includes 999 calls made to the emergency services and closed circuit television. In addition, personal data may also include special category data typically this includes data relating to: ● Health ● Race/Ethnicity ● Religious Beliefs, and Trade Union Membership Some special category data may relate to children. Additionally some personal data relating to criminal convictions and offences may also be processed.
Categories of Data Subject	Data subject categories typically include: ● Core Participants in the Inquiry, within the meaning of the Inquiries Act 2005; ● Other witnesses providing evidence to the Inquiry who are not core participants within the meaning of the Inquiries Act 2005, including Expert Witnesses appointed by the Inquiry; ● Members of the Public.

Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	Data will be retained until the Inquiry has concluded. Once this has occurred, data, including personal data, that is not required for archiving purposes will be destroyed. This destruction must be undertaken and confirmed by the Supplier to the Buyer in a manner which provides sufficient assurance that it has been completed satisfactorily and irrevocably. Some of the personal data held by the Inquiry will be transferred for the purposes of retention of Inquiry records by the National Archives in accordance with the UK Public Records Act 1958.

Part B **Joint Controller Agreement *(Optional)***

Not Used

Part C **Independent Controllers**

Not used

VII. Annex 2 – Specification

PURPOSE

- The authority is in the phase of finalising the Grenfell Tower Inquiry in its findings and publishing it. In order for this to be completed, this procurement is required to provide Counsels, the chair and the Panel members a platform for documents to be uploaded by all parties in order to hyperlink documents and transcripts already held on the platform. Transcription and EPE operator services will also be required for the report writing phase as well as ongoing work around the publication right up until the Phase 2 report.
- This will allow all parties to share and collaborate in a secure manner to write and publish the report as set out in the terms and conditions of the inquiry.

BACKGROUND TO THE CONTRACTING AUTHORITY

- The Grenfell Tower Inquiry was established in June 2017 under the terms of the Inquiries Act 2005, under the chairmanship of retired Appeal Court judge Sir Martin Moore-Bick. The Inquiry is independent of government and comprises: legal Counsel to the Inquiry; the Inquiry Secretary and his supporting staff, who are civil servants seconded to the Inquiry; and the

Inquiry Solicitor and her team, who are seconded to the Inquiry from the Government Legal Department, supplemented by contractors and agency staff (paralegals) as needed. Public inquiries are funded by the taxpayer given the overwhelming public interest in the matters they are invariably set up to consider and are sponsored by a government minister, in this case the Prime Minister. Once established, they are completely independent.

BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

- The Cabinet Office is seeking to establish a single Contract for the purchase of e-bundle services and access for the chair of the inquiry, panel members and counsel to share and collaborate on documents in producing and publishing the findings of the Grenfell Tower Inquiry in a secure manner. The report is to focus on documents that are based on heard evidence from hundreds of people and look at processes, procedures and regulations governing the construction, refurbishment, and management of high-rise premises.

DEFINITIONS

Expression or Acronym	Definition
CO	Cabinet Office
GTI	Grenfell Tower Inquiry

SCOPE OF REQUIREMENT

The Supplier shall be required to provide expertise in the development of services. The desired outcomes for this requirement are:

- Creation of runs of bundles under topics, e.g.
- “Plans related to topic X”;
- “Correspondence related to topic Y”;
- “materials testing data.”
- Bundles to be given topic-related letters, then numbers, then internally a page. Each bundle starts with page 1.
- All documents in the bundle have URN number as well as bundle number.
- Easy export of disclosed and redacted documents held on the Relativity document management system into bundles at any time, with repagination using letters (so if a new 4 page document has to go behind page 123, it becomes page 123A-D).
- System for users to create:
- their own core or other bundle,
- or their own index, with hyperlinks in it.
- Pages to be highlightable and capable of carrying comments for viewing by other users, for xx preparation.
- System for hyperlinking documents into:
- (i) Word documents such as notes and reports, and ● (ii) the daily transcript.

- Easy cutting and pasting from documents into Word or other documents.
- Creation of bundle indices with proper document description plus date, URN and bundle page number.
- Accessible side bar on screens for showing the bundle run so one can jump about easily.
- Split screens so that users can view up to 4 documents at a time.
- System for magnifying and marking documents while on screen, or overlaying different documents for comparison, for example, showing amendments to draft documents.

THE REQUIREMENT

The contract deliverables for this requirement are:

- Maintain Opus Magnum site and fields/folders ● Maintain all Transcripts.
- Document uploads to Magnum via Epiq
- Transfer Platform uploads to Magnum including draft report chapters
- Cross checking spreadsheets of documents for broken link reports
- Upload of documents to website
- Realtime Transcription Service and EPE operator (subject to final decision on seminars in connection with recommendations or any final hearing to
- deliver/announce report). [Query with Counsel whether we still need Real Time functionality in connection with report writing]

KEY MILESTONES AND DELIVERABLES

The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	Hold initial Supplier - Client meeting: for Client to set out expectations for turnaround times required by the Client	Within week 1 of Contract Award
2	Hold Supplier - Client - existing Supplier meeting: to agree rules of engagement to deliver the service required in the process leading up to writing/publication of the inquiry.	Within week 1 of Contract Award
3	Continue with the bi-monthly contract monitoring meetings: to ensure Supplier is meeting all KPIs and quality expectations	Within week 2 of Contract Award

MANAGEMENT INFORMATION/REPORTING

- The Supplier will maintain and supply on a regular basis, and in any case at least 48 hours ahead of the bi-monthly contract review meetings, such management information as the

Authority may reasonably require to enable the Authority to monitor the performance of the Supplier against the contract requirements and to give feedback from the Authority.

- The Supplier will report progress to the Authority's Programme Manager who will be the one point of contact for the Supplier for support and to review progress.

VOLUMES

- E-bundle services for up to 100 users - variable rate according usage.
- E-Bundle access for up to 100 users- fixed rate

CONTINUOUS IMPROVEMENT

- The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
- Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

SUSTAINABILITY

- The Supplier should minimise impact on environmental sustainability by minimising landfill waste, paper, water, energy consumption and carbon emissions during delivery of the Contract.

QUALITY

- Effective and high standard quality assurance is a fundamental requirement for all work carried out by the Supplier.
- Suppliers should note the UK Government Service Standards can be referenced on this site: https://www.gov.uk/service-manual/service-standard

PRICE

- Prices must not exceed the budget of the services/goods.
- Pricing must be submitted as a Fixed Price Proposal as per the Digital Marketplace Briefing. This is including all expenses including Travel & Subsistence, which must be absorbed into the Supplier's Fix Price Proposal.
- The maximum budget available for this requirement is £130,000 (ex VAT).

STAFF AND CUSTOMER SERVICE

- The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

- The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
- The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

VIII. Annex 3 – Charges

The Charges for the Deliverables shall not exceed £130,000 + VAT

In line with G-Cloud and as outlined below, all fees and rates agreed in the previous Call-Off Contract (CCTS19A38) shall apply.

This estimate is based on assumptions provided by the Customer and is subject to change based on the requirements of the Inquiry.

Workspace Preparation Fees		**Cost**
	Hearing Bundle Uploads - £0.75 per document*. **Subject to a minimum of 4 users for a minimum access period of 4 weeks and additional conditions below.* The Workspace Preparation fees cover the initial ingestion of the documents only, and is exclusive of any content management including structuring, metadata application, application of any access control lists (ACL), additions, replacements, inserts, re ordering of documents, repurposing, re-structuring of folders, and sequential pagination, all of which are charged for at the hourly rate of £180 (out of standard business working hours will be charged at 1.5 times the applicable rate).	TBC
	In the event that additional work is required after the initial ingestion and creation of the Inquiry Workspace, an hourly content management fee will be charged - £180 per hour. Technical support will also be provided at the same rate, as required. Work conducted out of standard business working hours, charged at 1.5x applicable rate.	TBC
	Across the Inquiry an hourly project management fee will be charged - £250 per hour. Work conducted out of standard business working hours, charged at 1.5x applicable rate.	TBC
	Hearing Bundle hyperlinks: Automated hyperlinks - £1 per link. (Manual hyperlinks - £3 per link)	TBC
	User generated hyperlinks - Free of charge.	
	Creation of additional mirror workspaces - £400 per workspace *3 workspaces are provided free of charge	TBC
Access Fees		**Cost**

	Access fees: - Magnum access licence - £7,000 per month for up to 100 users. Magnum access fees are payable from when Opus 2 first grants access to users.	TBC
	A minimum user access period of 2 weeks per user.	
Additional Benefits		**Cost**
	Storage of documents on a private UK server.	Free of charge
	Training during standard business hours (9.00am to 6.00pm, Monday to Friday) -£180 per hour Any travel fares and expenses - charged at cost.	TBC
TOTALS		**Cost**
		TBC
Magnum Cancellation Fees		**Cost**
	All Magnum fees incurred to date of Magnum services being cancelled will be charged accordingly.	Fees to date

Attendance Fees Cost Sitting Hours of up to 5½ hours - £840 per day. TBC

	Additional Sitting Hours - £105 per half hour*. If the Sitting Hours meet or exceed 8 hours, two daily attendance fees will be charged in place of overtime. ****Should the hearing be likely to exceed 5½ hours, please consult us in advance to ensure availability.***	TBC
Realtime Services		**Cost**
	1-25 connections - £135 per connection. 26-50 connections - £75 per connection 51+ connections - £50 per connection Each connection includes complimentary use of a laptop or iPad. ***Minimum of 5 chargeable connections.***	TBC
Electronic Presentation of Evidence (EPE) & On-site Technical Support		**Cost**
	EPE Operator, inclusive of 10 evidence display screens - £495 per day. Additional screens available upon request.	TBC

Set-up Fees		**Cost**
	EPE set-up and configuration - £1,000 per set-up. Payable 2 weeks in advance of the hearing.	TBC
	Preparation and configuration of local server for hearing room - £2,000 per set-up. Payable 2 weeks in advance of the hearing.	TBC
Optional Extras		**Cost**
	Hardcopy transcripts - £35 per copy.	TBC if required
	Email in Word format as required during the lunch break for distribution and publication to the Inquiry website - £150 per day.	TBC
Additional Benefits		**Cost**
	ASCII and Word formats.	Free of charge
	Adobe Acrobat PDF (Condensed with word index) as standard.	
	Audio synchronised to the transcript at the end of the day.	Free of charge

	Dedicated Case Manager throughout the hearing.	Free of charge
	Training during standard business hours (9.00am to 6.00pm, Monday to Friday)	Free of charge
TOTALS		**Cost**
		TBC
Hearing Room Services Cancellation Fees		**Cost**
	Transcription services cancelled before 10am, one working day prior to commencement.	Free of charge
	Transcription services cancelled after 10am, one working day prior to commencement.	£1,680
	Individual Sitting Days (if cancelled after 10am on preceding working day).	£840
	If an individual Sitting Day is cancelled after 10am on the working day before EPE Operator is due to sit.	£495

IX.Annex 4 – Supplier Tender

Not Used

X. Annex 5 – Optional IPR Clauses

Not Used

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

Not Used

Part B **Supplier ownership of New IPR with Buyer rights for the current Contract and broader public sector functions**

Not Used

XI. Annex 6 - Security Management

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 3)		
The Supplier must have the following Certifications:	ISO/IEC 27001:2013 by a UKAS-approved certification body	☒
	Cyber Essentials Plus	☒
	Cyber Essentials	☐
Subcontractors that Process Government Data must have the following Certifications:	ISO/IEC 27001:2013 by a UKAS-approved certification body	☐
	Cyber Essentials Plus	☒
	Cyber Essentials	☐
Locations (see Paragraph 4)		
The Supplier and Subcontractors may store, access or Process Government Data in:	the United Kingdom only	☒
	the United Kingdom and European Economic Area only	☐
	anywhere in the world not prohibited by the Buyer	☐

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.

Security testing (see Paragraph 9)

The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☒
Cloud Security Principles (see Paragraph 10)	

The Supplier must assess the Supplier System against the Cloud Security Principles	☒
Record keeping (see paragraph 11)	
The Supplier must keep records relating to Subcontractors, Sites, Third Party Tools and third parties	☒
Encryption (see Paragraph 12)	
The Supplier must encrypt Government Data while at rest or in transit	☒
Protecting Monitoring System (see Paragraph 13)	
The Supplier must implement an effective Protective Monitoring System	☒
Patching (see Paragraph 14)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☒
Malware protection (see Paragraph 15)	
The Supplier must use appropriate Anti-virus Software	☒
End-user Devices (see Paragraph 16)	
The Supplier must manage End-user Devices appropriately	☒
Vulnerability scanning (see Paragraph 17)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☒

Access control (see paragraph 18)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	☒
Return and deletion of Government Data (see Paragraph 19)	
The Supplier must return or delete Government Data when requested by the Buyer	☒
Physical security (see Paragraph 20)	
The Supplier must store Government Data in physically secure locations	☒
Security breaches (see Paragraph 21)	
The Supplier must report any Breach of Security to the Buyer promptly	☒
Security Management Plan (see Paragraph 22)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected have been met.	☒

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

	removes the Malicious Software from the Supplier System;
"Contract Year"	means: a period of 12 months commencing on the Effective Date; thereafter a period of 12 months commencing on each anniversary of the Effective Date; 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;
"Government Data"	means any: 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; Personal Data for which the Buyer is a, or the, Data Controller; or any meta-data relating to categories of data referred to in paragraphs (a) or (b);

	that is: supplied to the Supplier by or on behalf of the Buyer; or that the Supplier generates, processes, stores or transmits under this Agreement; and for the avoidance of doubt includes the Code and any meta-data relating to the Code.
"Certifications"	means one or more of the following certifications:

	ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and Cyber Essentials Plus; and/or Cyber Essentials;
"Breach of Security"	means the occurrence of: any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data; the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or any part of the Supplier System ceasing to be compliant with the required Certifications; the installation of Malicious Software in the Supplier System: 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 includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or was undertaken, or directed by, a state other than the United Kingdom;
"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: has been certified by the NCSC; holds "Green Light" status; and is authorised to provide the IT Health Check services required by Paragraph 5.2 (*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.
"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;
"End-user Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
"IT Health Check"	means testing of the Supplier Information Management System by a CHECK Service Provider;
"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 Information Management System, or substantially similar access privileges;

"Process"	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;
"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;
"Sites"	means any premises (including the Buyer's Premises, the Supplier's premises or third party premises): from, to or at which: the Services are (or are to be) provided; or the Supplier manages, organises or otherwise directs the provision or the use of the Services; or where: any part of the Supplier System is situated; or any physical interface with the Authority System takes place;
"Standard Contractual Clauses"	means, for the purposes of this Annex 6 (*Security Management*): the standard data protection paragraphs specified in Article 46 of the UK GDPR setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area;

	as modified to apply equally to the Government Data as if the Government Data were Personal Data;
"Subcontractor Personnel"	means: any individual engaged, directly or indirectly, or employed, by any Subcontractor; and engaged in or likely to be engaged in: the performance or management of the Services; or the provision of facilities or services that are necessary for the provision of the Services;

"Supplier System"	means any: information assets, IT systems, IT services; or Sites, that the Supplier or any Subcontractor will use to Process, or support the Processing of, Government Data and provide, or support the provision of, the Services; and the associated information management system, including all relevant: organisational structure diagrams; controls; policies; practices; procedures; processes; and resources;

"Third-party Tool"	means any activity conducted other than by the Supplier during which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

Part One: Core Requirements

3 Certification Requirements

3.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Process Government Data are certified as compliant with Cyber Essentials.

3.2 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:

3.3 The Supplier must ensure that the specified Certifications are in place for it and any relevant

Subcontractor: (a) before the Supplier or any Subcontractor Processes Government Data; and (b)

throughout the Term.

4 Location

4.1 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 Process Government Data outside the United Kingdom.

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

4.3 Where the Buyer has permitted the Supplier and its Subcontractors to store, access or process Government Data outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Subcontractors store, access or process 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 an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

(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 Sub-contractor will store, access, manage and/or Process the Government Data as required by this Annex 6 (*Security Management*);

(d) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

4.4 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**").

4.5 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.

5 Staff vetting

5.1 The Supplier must not allow Supplier Personnel, and must ensure that Subcontractors do not allow Subcontractor Personnel, to access or Process 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 HMG Baseline Personnel Security Standard (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) has not undergone national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify

6 Supplier assurance letter

6.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its chief technology officer (or equivalent officer) 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 Agreement;

(b) it has fully complied with all requirements of this Annex 6 (*Security Management*); and

(c) all Subcontractors have complied with the requirements of thisAnnex 6 (*Security Management*)) with which the Supplier is required to ensure they comply;

(d) the Supplier considers that its security and risk mitigation procedures remain effective.

7 Assurance

7.1 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 6 (*Security Management*).

7.2 The Supplier must provide that information and those documents:

(a) within 10 Working Days of a request by the Buyer;

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

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

8 Use of Subcontractors and third parties

8.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Process Government Data comply with the requirements of this Annex 6 (*Security Management*).

Part Two: Additional Requirements

9 Security testing

9.1 The Supplier must:

(a) before Processing 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 9.2; and

(d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 9.3.

9.2 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.

9.3 The Supplier treat any vulnerabilities as follows:

(a) the Supplier must remedy any vulnerabilities classified as critical 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 9.3(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 9.3(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 Heath Check report:

(i) if it is technically feasible to do so, within 3 months 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 9.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(d) 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.

10 Cloud Security Principles

10.1 The Supplier must ensure that the Supplier Solution complies with the Cloud Security Principles.

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

(a) before Processing Government Data;

(b) at least once each Contract Year; and

(c) when required by the Buyer.

10.3 The Supplier must:

(a) keep records of any assessment that it makes under Paragraph 10.2; and

(b) provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

11 Information about Subcontractors, Sites, Third Party Tools and third parties

11.1 The Supplier must keep the following records:

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

(i) 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:

(1) country of registration;

(2) registration number (if applicable); and

(3) registered address;

(ii) the Relevant Certifications held by the Subcontractor or third party;

(iii) the Sites used by the Subcontractor or third party;

(iv) the Services provided or activities undertaken by the Subcontractor or third party;

(v) the access the Subcontractor or third party has to the Supplier System;

(vi) the Government Data Processed by the Subcontractor or third party; and

(vii) the measures the Subcontractor or third party has in place to comply with the requirements of this Annex 6 (*Security Management*).

(b) for Sites from or at which Government Data is accessed or Processed:

(i) the location of the Site;

(ii) 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);

(iii) the Relevant Certifications that apply to the Site;

(iv) the Government Data stored at, or Processed from, the site; and

(c) for Third Party Tools:

(i) the name of the Third Party Tool;

(ii) the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

(iii) 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.

11.2 The Supplier must update the records it keeps in accordance with Paragraph 11.1:

(a) at least four times each Contract Year;

(b) whenever a Subcontractor, third party that accesses or Processes Government Data, Third Party Tool or Site changes; or

(c) whenever required to go so by the Buyer.

11.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 11.1 to the Buyer within 10 Working Days of any request by the Buyer.

12 Encryption

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

(a) when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

(b) when transmitted.

13 Protective monitoring system

13.1 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**").

13.2 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:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Government Data; and

(c) the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

14 Patching

14.1 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":

(i) if it is technically feasible to do so, within 5 Working Days 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 14.1(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 14.1(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 14.1(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.

15 Malware protection

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

15.2 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 (i) prevents the harmful effects from the Malicious Software; and (ii) removes the Malicious Software from the Supplier System.

16 End-user Devices

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

(a) the operating system and any applications that store, process 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-under 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 Suppler 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.

16.2 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 Agreement.

17 Vulnerability scanning

17.1 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.

18 Access control

18.1 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.

18.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier Information Management 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:

(i) restricted to a single role or small number of roles;

(ii) time limited; and

(iii) restrict the Privileged User's access to the internet.

19 Return and deletion of Government Data

19.1 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.

20 Physical security

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

21 Breach of security

21.1 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.

22 Security Management Plan

22.1 This Paragraph 22 applies only where the Buyer has selected this option in paragraph 1.3.

Preparation of Security Management Plan

22.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Annex 6 (*Security Management*) and the Agreement in order to ensure the security of the Supplier solution and the Buyer data.

22.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Agreement, the Security Management Plan, which must include a description of how all the options selected in this schedule are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 3.

Approval of Security Management Plan

22.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

(a) an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

22.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

22.6 The rejection by the Buyer of a revised Security Management Plan is a material Default of this Agreement.

Updating Security Management Plan

22.7 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

Monitoring

22.8 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Supplier Information Management System;

(b) a new risk to the components or architecture of the Supplier Information Management System;

(c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

(g) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(h) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

22.9 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.