SHORT FORM CONTRACT FOR THE SUPPLY OF SERVICES

Order Form

1. Contract Reference	
2. Date	26 June 2024
3. Buyer	Infected Blood Inquiry of Aldwych House, 5th Floor, 71-91 Aldwych, London, WC2B 4HN
4. Supplier	The British Red Cross incorporated and registered in England and Wales with charity number 220949 whose registered address is, 44 Moorfields, London, EC2A 9AL
5. The Contract	The Supplier shall supply the deliverables described below on the terms set out in this Order Form and the attached contract conditions ("**Conditions**") and **Annexes**. Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in Conditions. In the event of any conflict between this Order Form and the Conditions, this Order Form shall prevail.

6. Deliverables	The Services are set out in Annex 1 and should be delivered in accordance with the specification and the conditions.

7. Specification	The specification of the Deliverables is as set out in Annex 1.
8. Start Date	02 July 2024
9. Expiry Date	30 September 2024
10. Extension Period	The Inquiry is due to conclude by the end of this contract however the Buyer may extend the Contract for a period of up to 3 months by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The terms and conditions of the Contract shall apply throughout any such extended period.
11. Charges	The Charges for the Deliverables shall be as set out below in Annex 2.

12. Payment	All invoices must be sent, quoting a valid purchase order number (PO Number), to: REDACTED TEXT under FOIA Section 40, Personal Information Within **10** Working Days of receipt of your countersigned copy of this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your Buyer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. Payments will be made to the supplier by: Bankers' Automated Clearing System (BACS). If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to APinvoices-CAB-u@gov.sscl.com
13. Buyer Authorised Representative	For general liaison your contact will continue to be REDACTED TEXT under FOIA Section 40, Personal Information
14. Supplier Authorised Representative (s)	For general liaison your contact will continue to be REDACTED TEXT under FOIA Section 40, Personal Information

15. Supplemental requirements in addition to the Short form Terms	Within the scope of the Contract, the Supplier will need to agree to Annex 3 - Security Schedule.

16. Address for notices	**Buyer:** Infected Blood Inquiry, Aldwych House, 5th Floor, 71-91 Aldwych, WC2B 4HN Attention: REDACTED TEXT under FOIA Section 40, Personal Information **Supplier:** British Red Cross, 44 Moorfields, London, EC2A 9AL London,
17. Key Personnel	**Buyer:** Infected Blood Inquiry, Aldwych House, 5th Floor, 71-91 Aldwych, WC2B 4HN REDACTED TEXT under FOIA Section 40, Personal Information **Supplier:** British Red Cross, 44 Moorfields, London, EC2A 9AL London,

18. Procedures and Policies	For the purposes of this Contract: The Buyer's Staff Vetting Procedures are: • The Buyer requires the Supplier to ensure that any person employed in the Delivery of the Deliverables has to at least Baseline Personnel Security Standard (BPSS) clearance as set out in the Cabinet Office HMG Baseline Personnel Security Standard Guidance available at Government baseline personnel security standard - GOV.UK (www.gov.uk) as it is replaced or amended from time to time. The Supplier shall ensure that no person who discloses that he/she has 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.

Signed - via Docusign

Supplier

<Supplier Sign Here>

Buyer

<Commercial Sign Here>

Annex 1 – Specification

1. PURPOSE

1. The Infected Blood Inquiry is seeking a provider of confidential psychological support for people affected by treatment with infected blood. This provider will provide both face-to face support at the Inquiry's public hearings and phone support on a dedicated helpline throughout the course of the Inquiry.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

1. The Inquiry is examining why men, women and children in the UK were given infected blood and/or infected blood products in the 1970s and 1980s, which caused HIV or hepatitis C; the impact on their families; the response by the authorities, including government; the nature of any support provided following infection; and whether there was a cover up.
2. The Inquiry is independent of government and sponsored by the Cabinet Office. For further details, including the terms of reference, please see the website www.infectedbloodinquiry.org.uk

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

1. During the Inquiry's preliminary hearings in September 2018, the Chair, Sir Brian Langstaff, set out six principles for how the Inquiry would carry out its work: people, thoroughness, respect, openness and transparency, independence and listening. As part of putting people affected at the heart of the Inquiry, Sir Brian recognised that giving evidence can be traumatic and committed the Inquiry to working in a sensitive manner.

2. Engaging in the Inquiry (although welcomed by many) is causing significant psychological distress for people affected. It is likely that this has been exacerbated by the long period of time since the original infection and by the reaction of others (including government organisations) since that time.

3. The Inquiry has been providing confidential psychological support for people affected by treatment with infected blood since the preliminary hearings. The Inquiry is now in its final stages and requires this service to be continued from 02 July 2024 (when the current contract ends) to 30 September 2024 when the Inquiry expects to conclude.

4. DEFINITIONS

1. Not applicable.

5. SCOPE OF REQUIREMENT

1. The requirement is for:
    1. A small number of fully qualified psychological practitioners (who have developed an understanding of the issues affecting people participating in the Inquiry) to attend the final day of public hearings in London (see 3.1).

    2. A small number of fully qualified psychological practitioners (who have developed an understanding of the issues affecting people participating in the Inquiry) to staff a confidential phone support line throughout the course of the Inquiry. The times at which the phone line is available are flexible, and subject to discussion with the Authority.

6. THE REQUIREMENT

1. Face to face psychological support will be required for one day in total (with private rooms made available by the Authority) at the final event in London.

2. The current confidential phone line contract is due to end on 02 July 2024. The new arrangements should be put in place so that this support can be continued seamlessly until the end of the Inquiry.

3. The provider will have regular monthly meetings (either by phone or in person as is convenient for both parties) with the Authority in relation to the phone line to discuss volumes, common themes, and any proposals for an improved service.

7. KEY MILESTONES AND DELIVERABLES

1. The following Contract milestones shall apply:

lileston	Description	Timeframe
1	Provider to allocate experienced practitioners to the contract.	Prior to contract commencement date
2	Identification of phone number and call times for the confidential support line.	
3	Provider to meet with the Deputy Secretary to review service provision to date and agree any adjustments to the approach going forward.	Every two months

8. MANAGEMENT INFORMATION/REPORTING

1. The provider should provide:

    1. A brief report following each week of hearings, with the key themes and numbers using the service, and

    2. A monthly report of call volumes and any specific concerns, with ad hoc reporting where issues of significant concern are raised, or additional briefing is required from the Authority.

9. VOLUMES

1. Around 2,000 core participants and several hundred other affected people are actively involved in the Inquiry. These people were either infected themselves, have lost a member of their family because of the damage caused by treatment with infected blood, or are currently caring for a family member who was infected.

10. CONTINUOUS IMPROVEMENT

1. The provider will have regular discussions with the deputy secretary to ensure that any suggestions to improve the service are implemented swiftly. The provider will provide management information (as outlined in 8.1) to inform these discussions.

2. Consistency of approach in the support provided is vital. Everyone using this service should receive a timely, professional and supportive service.

3. Changes to the way in which the Services are to be delivered must be brought to the deputy secretary's attention and agreed prior to any changes being implemented.

11. SUSTAINABILITY

1. Not applicable.

12. QUALITY

1. The practitioners must be professionally qualified and experienced, and provide a consistent approach. The service will be confidential and non-judgemental, and demonstrate an understanding of the effects of living with the physical, psychological and emotional damage caused by treatment with infected blood.

13. PRICE

1. The phone support provision will be charged at £REDACTED TEXT under FOIA Section 43 (2), Commercial Information

2. Prices for the final presentation is £REDACTED TEXT under FOIA Section 43 (2), Commercial Information

14. STAFF AND CUSTOMER SERVICE

1. Providers staff assigned to the telephone support line must have the relevant qualifications and experience, including an understanding of the issues affecting people treated with infected blood.

15. SERVICE LEVELS AND PERFORMANCE

1. The Authority will measure the quality of the provider's delivery by:

SLA	Service Area	SLA description	Target
1	**Service Quality** - Resourcing & Service Delivery	All staff working on the contract must have completed the provider's DBS requirements.	100%
2		Availability of psychological support throughout the hearings	100%
3	**Service Quality** - Feedback	Positive feedback (and lack of complaints) on the service from people affected by the treatment with infected blood	Ongoing
4	**DeliveryTimescale** - Live calls	Response received to calls made during agreed "live" helpline hours	99%
5	**Service Delivery** - Responses to messages	Messages received for call backs to be returned on the same working day	90%
6		Messages received "out of hours" replied to on the next working day	90%

7	**Service Delivery** – Continual improvement	Provider to meet with the Inquiry Team to review service provision to date and agree any adjustments to the approach going forward.	Every Two months

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

1. All staff working on the contract must have completed the provider's DBS requirements.

17. PAYMENT AND INVOICING

1. Provider invoicing requirements will be in line with standard Cabinet Office processes. A Purchase Order will be set up by the Inquiry and the provider will invoice on a monthly basis.

2. Before payment can be considered, each invoice must include a detailed breakdown of work completed and the associated costs.

18. CONTRACT MANAGEMENT

1. The provider shall meet with the Authority every two months upon commencement of the contract. The purpose of these meetings will be to review service provision to date and to agree any adjustments to the approach going forward in line with SLA number 7, detailed in Section 15 of this Statement of Requirements.

2. Attendance at Contract Review meetings shall be at the provider's own expense.

19. LOCATION

1. The location of the Services will be carried out as follows:

1. Psychological support via a confidential phone line.

2. Face to face psychological support during the final presentation in London.

Annex 2 – Charges

The phone line service will cost £REDACTED TEXT under

FOIA Section 43 (2), Commercial Information

The price for the final presentation is £ REDACTED TEXT

under FOIA Section 43 (2), Commercial Information.

Annex 3 – Security Schedule

1 Supplier obligations

Core requirements

1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 8.

1.2 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Certifications (see Paragraph 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 (ii)removes the Malicious Software from the Supplier System;

"Contract Year"	means: (a) a period of 12 months commencing on the Effective Date; (b) thereafter a period of 12 months commencing on each anniversary of the Effective Date; (c) 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: (a) 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; (b) Personal Data for which the Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in paragraphs (a) or (b); that is: (d) supplied to the Supplier by or on behalf of the Buyer; or (e) that the Supplier 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: (b) 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 (c) Cyber Essentials Plus; and/or (d) Cyber Essentials;

"Breach of Security"	means the occurrence of: (a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data; (b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or (c) any part of the Supplier System ceasing to be compliant with the required Certifications; (d) the installation of Malicious Software in the Supplier System: (e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and (f) includes any attempt to undertake the activities listed in subparagraph (a) where the Supplier has reasonable grounds to suspect that attempt: (i) was part of a wider effort to access information and communications technology

	operated by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom;
"CHECK Scheme"	means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
"CHECK Service Provider"	means a company which, under the CHECK Scheme: (a) has been certified by the NCSC; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by Paragraph 6 (*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 securityguidance;
"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): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Authority System takes place;
"Standard Contractual Clauses"	means, for the purposes of this Schedule [◆] (*Security Management*): (a) 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; (b) as modified to apply equally to the Government Data as if the Government Data were Personal Data;
"Subcontractor Personnel"	means: (a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and (b) engaged in or likely to be engaged in: (i) the performance or management of the Services; or (ii) the provision of facilities or services that are necessary for the provision of the Services;
"Supplier System"	means (a) any:

	(i) information assets, (ii) IT systems, (iii) IT services; or (iv) Sites, that the Supplier or any Subcontractor will use to Process, or support the Processing of, Government Data and provide, or support the provision of, the Services; and (b) the associated information management system, including all relevant: (i) organisational structure diagrams; (ii) controls; (iii) policies; (iv) practices; (v) procedures; (vi) processes; and (vii) resources;
"Third-party Tool"	means any 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 Schedule [◆] (*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 Schedule [◆] (Security Management); and

(c) all Subcontractors have complied with the requirements of this Schedule [◆] (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 Schedule [◆] (*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 Schedule [◆] (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.

10.1 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 Schedule [◆] (*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) (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 Schedule [♦] (*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.

Short form Terms

1. Definitions used in the Contract

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

"Central Government Body" means a body listed in one of the following subcategories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;	

"Charges" means the charges for the Deliverables as specified in the Order Form; **"Confidential Information"** means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;

"Contract" means the contract between (i) the Buyer and (ii) the Supplier which is created by the Supplier's counter signing the Order Form and includes the Order Form and Annexes;

"Controller" has the meaning given to it in the GDPR; letterhead of the Order Form;

"Buyer" means that date by which the **"Date of Delivery"** Deliverables must be delivered to the means the person identified in the Buyer, as specified in the Order Form;

"Buyer Cause" any breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Buyer is liable to the Supplier;

"Data Protection Legislation" Act 2018 to the extent that it relates to processing

of personal data and privacy; (iii) all applicable Law about the processing of

"Data Protection Impact Assessment" personal data and privacy; an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

"Data Protection Officer"
(i) the GDPR, the LED and any applicable national implementing Laws as amended has the meaning given to it in the GDPR; from time to time (ii) the Data Protection

"Data Subject" has the meaning given to it in the GDPR;

held by the Supplier under this Contract,

"Data Loss Event" and/or actual or potential loss and/or any event that results, or may result, in destruction of Personal Data in breach of unauthorised access to Personal Data this Contract, including any Personal Data Breach;

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 Access

"Deliver" means hand over the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and any other specific arrangements agreed in accordance with Clause [ ]. Delivered and Delivery shall be construed accordingly;

"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" means the date for expiry of the Contract as set out in the Order Form;

"FOIA" means 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" excluding: i) any industrial dispute any event, occurrence, circumstance, relating to the Supplier, the Supplier matter or cause affecting the Staff (including any subsets of them) or performance by

either Party of its Contract arising any other failure in the Supplier or the Subcontractor's supply chain; ii) any omissions, happenings event, occurrence, circumstance, matter or non-happenings beyond its or cause which is attributable to the control which prevent or wilful act, neglect or failure to take from performing its reasonable precautions against it by the the Contract but Party concerned; and iii) any failure of lack of funds; obligations under the delay caused by a

"GDPR" the General Data Protection Regulation (Regulation (EU) 2016/679);

"Goods" means the goods to be supplied by the Supplier to the Buyer under the Contract;

"Good Industry Practice" standards, practices, methods and procedures conforming to the law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;

"Government 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 Data Controller;

"Information" has the meaning given under section 84 of the FOIA;

"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; ii) 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); iii) if an administrator or administrative receiver is appointed in respect of the whole or any part of the persons assets or business; iv) if the person makes any composition with its creditors or 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;

"Key Personnel" means any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing;

"LED" Law Enforcement Directive (Directive (EU) 2016/680);

"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;

"Order Form" means the letter from the Buyer to the Supplier printed above these terms and conditions;

"Party" the Supplier or the Buyer (as appropriate) and "Parties" shall mean both of them;

"Personal Data" has the meaning given to it in the GDPR;

has the meaning given to it **"Personal Data Breach"** in the GDPR;

in the GDPR

order for

"Processor" has the meaning given to it

Purchase Order Number" means the Buyer's unique number relating to the Deliverables to be supplied by the Supplier to the Buyer in accordance with the terms of the Contract

;

"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 out for the term "request" shall apply); 2004 as relevant (where the meaning set

"Services" means the services to be supplied by the Supplier to the Buyer under the Contract;

"Specification" means 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" means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier's obligations under the Contract;

"Staff Vetting Procedures" means vetting procedures that accord with good industry practice

any third Party appointed to process Personal Data on behalf of the Supplier

"Subprocessor " related to the Contract;

"Supplier all directors, officers, employees, agents, **Staff"** consultants and contractors of the

or, where applicable, the Buyer's Supplier and/or of any Subcontractor procedures for the vetting of personnel as engaged in the performance of the provided to the Supplier from time to time; Supplier's obligations under a Contract;

"Supplier" means the person named as Supplier in the Order Form;

"Term" means the period from the start date of the Contract set out in the Order Form to the Expiry Date as such period may be extended in accordance with clause [ ] or terminated in accordance with the terms and conditions of the Contract;

"US-EU Privacy Shield Register" a list of companies maintained by the United States of America Department for Commence that have self-certified their commitment to adhere to the European legislation relating to the processing of personal data to non-EU countries which is available online at: https://www.privacyshield.gov/list;

"VAT" means value added tax in accordance with the provisions of the Value Added Tax Act 1994;

"Workers" 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/procurementpolicynote-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;

"Working Day" means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

2. Understanding the Contract

In the Contract, unless the context otherwise requires:

2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;

2.2 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;

2.3 the headings in this Contract are for information only and do not affect the interpretation of the Contract;

2.4 references to "writing" include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;

2.5 the singular includes the plural and vice versa;

2.6 a reference to any law includes a reference to that law as amended, extended, consolidated or re-enacted from time to time and to any legislation or byelaw made under that law; and

2.7 the word 'including', "for example" and similar words shall be understood as if they were immediately followed by the words "without limitation".

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 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

(a) The Supplier must provide Deliverables: (i) in accordance with the Specification; (ii) to a professional standard; (iii) using reasonable skill and care; (iv) using Good Industry Practice; (v) using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract; (vi) on the dates agreed; and (vii) that comply with all law.

(b) 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

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

(b) All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

(c) The Supplier transfers ownership of the Goods on completion of delivery (including off-loading and stacking) or payment for those Goods, whichever is earlier.

(d) 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 three Working Days of delivery.

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

(f) The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

(g) The Supplier must provide sufficient packaging for the Goods to reach the point of delivery safely and undamaged.

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

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

(j) 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.

(k) 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 steps to minimise these costs.

(l) 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.

(m) 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 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 [sub suppliers].

4.3 Services clauses

(a) Late delivery of the Services will be a default of the Contract.
(b) 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 any security requirements.
(c) The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services
(d) 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.
(e) The Supplier must allocate sufficient resources and appropriate expertise to the Contract.
(f) The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
(g) 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.
(h) The Supplier must ensure all Services, and anything used to deliver the Services, are of good quality [and free from defects].
(i) 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 shall be entitled to invoice the Buyer for the charges in the Order Form. The Supplier shall raise invoices promptly and in any event within 90 days from when the charges are due.

5.2 All Charges:

(a) exclude VAT, which is payable on provision of a valid VAT invoice; (b) include all costs 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 Order Form.

5.4 A Supplier invoice is only valid if it:

(a) includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer;
(b) includes a detailed breakdown of Deliverables which have been delivered (if any).

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 33.

5.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier 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: (a) the Buyer cannot terminate the Contract under clause 11;
(b) the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;
(c) the Supplier is entitled to additional time needed to deliver the Deliverables; (d) the Supplier cannot suspend the ongoing supply of Deliverables.

6.2 Clause 6.1 only applies if the Supplier:
(a) gives notice to the Buyer within 10 Working Days of becoming aware; (b) demonstrates that the failure only happened because of the Buyer Cause;
(c) 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 seven years after the date of expiry or termination of the Contract.

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

7.4 The Supplier must provide information to the auditor and reasonable co operation at their request.

7.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately: (a) tell the Buyer and give reasons;
(b) propose corrective action;
(c) provide a deadline for completing the corrective action.

7.6 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:

(a) 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

(b) 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).

8. Supplier staff

8.1 The Supplier Staff involved in the performance of the Contract must: (a) be appropriately trained and qualified;

(b) be vetted using Good Industry Practice and in accordance with the [instructions issued by the Buyer in the Order Form] [Staff Vetting Procedures]; (c) comply with all conduct requirements when on the Buyer's premises.

8.2 Where a 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 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach clause 8.

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

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

8.6 The Supplier shall use those persons nominated in the Order Form (if any) to provide the Deliverables and shall not remove or replace any of them unless:

(a) requested to do so by the Buyer (not to be unreasonably withheld or delayed);

(b) the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

(c) the person's employment or contractual arrangement with the Supplier or any subcontractor is terminated for material breach of contract by the employee.

9. Rights and protection

9.1 The Supplier warrants and represents that:

(a) it has full capacity and authority to enter into and to perform the Contract;

(b) the Contract is executed by its authorised representative;

(c) it is a legally valid and existing organisation incorporated in the place it was formed;

(d) 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;

(e) it maintains all necessary rights, authorisations, licences and consents to perform its obligations under the Contract;

(f) it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and (g) it is not impacted by an Insolvency Event.

9.2 The warranties and representations in 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: (a) wilful misconduct of the Supplier, any of its subcontractor and/or Supplier Staff that impacts the Contract; (b) non-payment by the Supplier of any tax or National Insurance.

9.4 If the Supplier becomes aware of a representation or warranty 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.

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 worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it and its sublicensees to both: (a) receive and use the Deliverables; (b) use the New IPR.

10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs for the purpose of fulfilling its obligations under the Contract and a perpetual, royalty-free, non-exclusive licence to use any New IPRs.

10.3 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.

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

10.5 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.

10.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

(a) obtain for the Buyer the rights in clauses 10.1 and 10.2 without infringing any third party intellectual property rights;

(b) 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.

11. Ending the contract

11.1 The Contract takes effect on the date of or (if different) the date specified in the Order Form and ends on the earlier of the date of expiry 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

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 11.5(b) to 11.5(g) applies.

11.4 When the Buyer can end the Contract

(a) 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:

(i) there's a Supplier Insolvency Event;

(ii) if the Supplier repeatedly breaches the Contract in a way to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Contract;

(iii) if the Supplier is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied; (iv) 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;

(v) if 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;

(vi) the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations;

(vii) the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them.

(b) If any of the events in 73(1) (a) to (c) of the Regulations (substantial modification, exclusion of the Supplier, procurement infringement) happen, the Buyer has the right to immediately terminate the Contract and clause 11.5(b) to 11.5(g) applies.

11.5 What happens if the Contract ends

Where the Buyer terminates the Contract under clause 11.4(a) all of the following apply:

(a) the Supplier is responsible for the Buyer's reasonable costs of procuring replacement deliverables for the rest of the term of the Contract;

(b) the Buyer's payment obligations under the terminated Contract stop immediately;

(c) accumulated rights of the Parties are not affected;

(d) the Supplier must promptly delete or return the Government Data except where required to retain copies by law;

(e) the Supplier must promptly return any of the Buyer's property provided under the Contract;

(f) 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;

(g) the following clauses survive the termination of the Contract: [3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35] and any clauses which are expressly or by implication intended to continue.

11.6 When the Supplier can end the Contract

(a) 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.

(b) If a Supplier terminates the Contract under clause 11.6(a):

(i) the Buyer must promptly pay all outstanding charges incurred to the Supplier;

(ii) 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;

(iii) clauses 11.5(d) to 11.5(g) apply.

11.7 Partially ending and suspending the Contract

(a) 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.

(b) 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.

(c) The Parties must agree (in accordance with clause 24) any necessary variation required by clause 11.7, but the Supplier may not either:

(i) reject the variation;

(ii) increase the Charges, except where the right to partial termination is under clause 11.3.

(d) 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:

(a) any indirect losses;

(b) 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: (a) its liability for death or personal injury caused by its negligence, or that of its employees, agents or subcontractors;

(b) its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;

(c) 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 4.2(j), 4.2(m), 8.5, 9.3, 10.5, 13.2, 14.26(e) or 30.2(b).

12.5 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.

12.6 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 must, in connection with provision of the Deliverables, use reasonable endeavours to:

(a) comply and procure that its subcontractors comply with the Supplier Code of

Conduct appearing at (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf) and such other corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time;

(b) support the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010;

(c) not use nor allow its subcontractors to use modern slavery, child labour or inhumane treatment;

(d) meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurement thegovernment-buying-standards-gbs

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 32

13.4 "Compliance Officer" the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;

14. Data protection

14.1 The Buyer is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation.

14.2 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with this Contract.

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

14.4 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every six Months.

14.5 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified [in writing] by the Buyer.

14.6 If at any time the Supplier suspects or has reason to believe that the Government Data provided under the Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Buyer and immediately suggest remedial action.

14.7 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:
(a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than five Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; (b) restore the Government Data itself or using a third party.

14.8 The Supplier must pay each Party's reasonable costs of complying with clause 14.7 unless the Buyer is at fault.

14.9 Only the Buyer can decide what processing of Personal Data a Supplier can do under the Contract and must specify it for the Contract using the template in Annex 1 of the Order Form (*Authorised Processing*).

14.10 The Supplier must only process Personal Data if authorised to do so in the Annex to the Order Form (*Authorised Processing*) by the Buyer. Any further written instructions relating to the processing of Personal Data are incorporated into Annex 1 of the Order Form.

14.11 The Supplier must give all reasonable assistance to the Buyer in the preparation of any Data Protection Impact Assessment before starting any processing, including:
(a) a systematic description of the expected processing and its purpose;
(b) the necessity and proportionality of the processing operations;
(c) the risks to the rights and freedoms of Data Subjects;
(d) the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.

14.12 The Supplier must notify the Buyer immediately if it thinks the Buyer's instructions breach the Data Protection Legislation.

14.13 The Supplier must put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Buyer.

14.14 If lawful to notify the Buyer, the Supplier must notify it if the Supplier is required to process Personal Data by Law promptly and before processing it.

14.15 The Supplier must take all reasonable steps to ensure the reliability and integrity of any Supplier Staff who have access to the Personal Data and ensure that they: (a) are aware of and comply with the Supplier's duties under this clause 11; (b) are subject to appropriate confidentiality undertakings with the Supplier or any Subprocessor;
(c) 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 Buyer or as otherwise allowed by the Contract;
(d) have undergone adequate training in the use, care, protection and handling of Personal Data.

14.16 The Supplier must not transfer Personal Data outside of the EU unless all of the following are true:
(a) it has obtained prior written consent of the Buyer;
(b) the Buyer has decided that there are appropriate safeguards (in accordance with Article 46 of the GDPR);
(c) the Data Subject has enforceable rights and effective legal remedies when transferred;
(d) the Supplier meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred;
(e) where the Supplier is not bound by Data Protection Legislation it must use its best endeavours to help the Buyer meet its own obligations under Data Protection Legislation; and
(f) the Supplier complies with the Buyer's reasonable prior instructions about the processing of the Personal Data.

14.17 The Supplier must notify the Buyer immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
(e) 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; (f) becomes aware of a Data Loss Event.

14.18 Any requirement to notify under clause 14.17 includes the provision of further information to the Buyer in stages as details become available.

14.19 The Supplier must promptly provide the Buyer with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.17. This includes giving the Buyer:

(a) full details and copies of the complaint, communication or request; (b) reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
(c) any Personal Data it holds in relation to a Data Subject on request;
(d) assistance that it requests following any Data Loss Event;
(e) assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office.

14.20 The Supplier must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Supplier employs fewer than 250 staff, unless either the Buyer determines that the processing: (a) is not occasional;

(b) includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR;
(c) is likely to result in a risk to the rights and freedoms of Data Subjects.

14.21 The Supplier must appoint a Data Protection Officer responsible for observing its obligations in this Schedule and give the Buyer their contact details.

14.22 Before allowing any Subprocessor to process any Personal Data, the Supplier must:

(a) notify the Buyer in writing of the intended Subprocessor and processing; (b) obtain the written consent of the Buyer;
(c) enter into a written contract with the Subprocessor so that this clause 14 applies to the Subprocessor;
(d) provide the Buyer with any information about the Subprocessor that the Buyer reasonably requires.

14.23 The Supplier remains fully liable for all acts or omissions of any Subprocessor.

14.24 At any time the Buyer can, with 30 Working Days notice to the Supplier, change this clause 14 to:

(a) replace it with any applicable standard clauses (between the controller and processor) or similar terms forming part of an applicable certification scheme under GDPR Article 42;
(b) ensure it complies with guidance issued by the Information Commissioner's Office.

14.25 The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner's Office.

14.26 The Supplier:

(a) must provide the Buyer with all Government Data in an agreed open format within 10
Working Days of a written request;
(b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
(c) must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
(d) 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;
(e) indemnifies the Buyer against any and all Losses incurred if the Supplier breaches clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

(a) keep all Confidential Information it receives confidential and secure; (b) 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;

(c) 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:

(a) where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
(b) if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;
(c) if the information was given to it by a third party without obligation of confidentiality;
(d) if the information was in the public domain at the time of the disclosure; (e) if the information was independently developed without access to the disclosing Party's
Confidential Information;
(f) to its auditors or for the purposes of regulatory requirements;
(g) on a confidential basis, to its professional advisers on a need-to-know basis;
(h) 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 Staff must enter into a direct confidentiality agreement with the Buyer at its request.

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

(a) on a confidential basis to the employees, agents, consultants and contractors of the Buyer;
(b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;
(c) if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
(d) where requested by Parliament; (e) 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 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 steps 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 Within the required timescales the Supplier must give the Buyer full co-operation and information needed so the Buyer can:

(a) comply with any Freedom of Information Act (FOIA) request;

(b) comply with any Environmental Information Regulations (EIR) request.

16.3 The Buyer 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, which does not need to be reasonable.

17. Invalid parts of the contract

If any part of the Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in a contract

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:

(a) provides written notice to the other Party;

(b) uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 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.

20.3 Where a Party terminates under clause 20.2: (a) each party must cover its own losses; (b) clause 11.5(b) to 11.5(g) applies.

21. Relationships created by the contract

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

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 the Contract 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.

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

a) their name;

(b) the scope of their appointment;
(c) the duration of their appointment.

24. Changing the contract

24.1 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.

25. How to communicate about the contract

25.1 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 when sent unless an error message is received.

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

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

26. Preventing fraud, bribery and corruption

26.1 The Supplier shall not:

(a) commit any criminal offence referred to in the Regulations 57(1) and 57(2); (b) 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.

26.2 The Supplier shall take all reasonable steps (including creating, maintaining and enforcing adequate policies, procedures and records), in accordance with good industry

practice, to prevent any matters referred to in clause 26.1 and any fraud by the 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.

26.3 If the Supplier or the Staff engages in conduct prohibited by clause 26.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Buyer) the Buyer may:

(a) terminate the Contract and recover from the Supplier the amount of any loss suffered by the Buyer resulting from the termination, including the cost reasonably incurred by the Buyer of making other arrangements for the supply of the Deliverables and any additional expenditure incurred by the Buyer throughout the remainder of the Contract; or

(b) recover in full from the Supplier any other loss sustained by the Buyer in consequence of any breach of this clause.

27. Equality, diversity and human rights

27.1 The Supplier must follow all applicable equality law when they perform their obligations under the Contract, including:

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

(b) any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

27.2 The Supplier must take all necessary steps, 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.

28. Health and safety

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

(a) all applicable law regarding health and safety;

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

28.2 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.

29. Environment

29.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

29.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

30. Tax

30.1 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.

30.2 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 Off Contract, the Supplier must both:

(a) 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;

(b) 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 Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

30.3 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 the following requirements:

(a) the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 30.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;

(b) 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;

(c) 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 30.2 or confirms that the Worker is not complying with those requirements;

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

31. Conflict of interest

31.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential 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.

31.2 The Supplier must promptly notify and provide details to the Buyer if a conflict of interest happens or is expected to happen.

31.3 The Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential conflict of interest.

32. Reporting a breach of the contract

32.1 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 26 to 31.

32.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 32.1.

33. Resolving disputes

33.1 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.

33.2 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 33.3 to 33.5.

33.3 Unless the Buyer refers the dispute to arbitration using clause 33.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

(a) determine the dispute;

(b) grant interim remedies;

(c) grant any other provisional or protective relief.

33.4 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.

33.5 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 33.3, 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 33.4.

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

34. Which law applies

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