**Digital Craftsmen Limited**
Suite 102,
254 Pentonville Road,
London
N1 9JY

Attn: Redacted Under FOIA Section 40, Personal Information
By email to: Redacted Under FOIA Section 40, Personal Information

Date: 18/08/2023
Your ref: GTI-DC-01

Dear Redacted Under FOIA Section 40, Personal Information

**Award of contract for the Provision of Website Maintenance, Hosting and Development**

Following your proposal for the supply of Website Maintenance, Hosting and Development to the Grenfell Tower Inquiry, we are pleased to confirm our intention to award this contract to you.

The attached contract details ("**Order Form**"), contract conditions and the [***Annexes***] set out the terms of the contract between the Grenfell Tower Inquiry for the provision of the deliverables set out in the Order Form.

We thank you for your cooperation to date, and look forward to forging a successful working relationship resulting in a smooth and successful delivery of the deliverables. Please confirm your acceptance of the Conditions by signing and returning the Order Form to Redacted Under FOIA Section 40, Personal Information at the above address within 7 days from the date of this Order Form. No other form of acknowledgement will be accepted. Please remember to include the reference number above in any future communications relating to this contract. We will then arrange for the Order Form to be countersigned which will create a binding contract between us.
Yours faithfully,

Redacted Under FOIA Section 40, Personal Information

**SHORT FORM CONTRACT FOR THE SUPPLY OF SERVICES**

# Order Form

| | | |
|---|---|---|
| **1. Contract Reference** | GTI-DC-01 | |
| **2. Date** | 18/08/2023 | |
| **3. Buyer** | Grenfell Tower Inquiry of 1 Giltspur Street, London, EC1A 9DD | |
| **4. Supplier** | Digital Craftsmen Limited<br>Suite 102,<br>253 Pentonville Road<br>London<br>N1 9JY<br>**Company Number:** 04423496 | |
| **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 any ***Annexes***.<br><br>Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in Conditions.<br><br>In the event of any conflict between this Order Form and the Conditions, this Order Form shall prevail.<br><br>Please do not attach any Supplier terms and conditions to this Order Form as they will not be accepted by the Buyer and may delay the conclusion of the Contract. | |
| **6. Deliverables** | **Goods** | [None] |

| | | |
|---|---|---|
| | **Services** | Provide services as set out in **Annex 2.** |
| **7. Specification** | The specification of the Deliverables is as set out in **Annex 2.** | |
| **8. Term** | The Term shall commence on 22/04/2023 and the Expiry Date shall be 27/06/2024 unless it is otherwise extended or terminated in accordance with the terms and conditions of the Contract. | |
| **9. Charges** | The Charges for the Deliverables are set out in and **Annex 3** and are as follows:<br><br>A fixed cost of £38,556 + VAT. | |

| | |
|---|---|
| **10. Payment** | Payment can only be made following satisfactory delivery of the preagreed certified deliverables. The proposed invoice schedule is outlined in **annex 3.**<br><br>All invoices must be sent, quoting a valid purchase order number<br><br>(PO Number), to: apinvoices-cab-u@gov.sscl.com copying in<br><br>finance@grenfelltowerinquiry.org.uk Hard copies can be sent to:<br><br>1 Giltspur Street, London, EC1A 9DD<br><br>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.<br><br>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.<br><br>If you have a query regarding an outstanding payment please contact our Accounts Payable section by email to finance@grenfelltowerinquiry.org.uk |
| **11. Buyer Authorised Representative(s)** | For general liaison your contacts will continue to be:<br><br>Redacted Under FOIA Section 40, Personal Information<br>and,<br><br>Redacted Under FOIA Section 40, Personal Information |

| | | |
|---|---|---|
| **12. Address for notices** | **Buyer**: Grenfell Tower Inquiry<br>**Attention:** Redacted Under FOIA Section 40, Personal Information<br>1 Giltspur Street,<br>London,<br>EC1A 9DD **Email**:<br>Redacted Under FOIA Section 40, Personal Information | **Supplier**: Digital Craftsmen Limited<br>**Attention:** Redacted Under FOIA Section 40, Personal Information<br>Digital Craftsmen Limited<br>Suite 102, 254 Pentonville Road, London<br>N1 9JY<br>**Email**:<br>Redacted Under FOIA Section 40, Personal Information |
| **13. Key Personnel** | Redacted Under FOIA Section 40, Personal Information<br>Grenfell Tower Inquiry<br>1 Giltspur Street,<br>London,<br>EC1A 9DD **Email**:<br>Redacted Under FOIA Section 40, Personal Information | Redacted Under FOIA Section 40, Personal Information<br>Digital Craftsmen Limited<br>Suite 102, 254 Pentonville Road, London<br>N1 9JY<br>**Email**:<br>Redacted Under FOIA Section 40, Personal Information |

| | |
|---|---|
| **14. Procedures and Policies** | For the purposes of the Contract the:<br><br>Cabinet Office's Staff Vetting Procedures are:<br><br>The Buyer requires the Supplier to ensure that any person employed in the Delivery of the Deliverables has undertaken a Disclosure and Barring Service (DBS) check.<br><br>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.<br><br>Please see Annex 4 - Security Schedule<br><br>Cabinet Office's additional sustainability requirements can be found in the following link:<br><br>https://www.gov.uk/government/publications/cabinet-office-environmental |

| | |
|---|---|
| | -policy-statement/cabinet-office-environmental-policy-statement<br><br>Cabinet Office's equality and diversity policy can be found at:<br><br>https://www.gov.uk/government/organisations/cabinet-office/about/equality-and-diversity |
| **15. Incorporated Terms** | The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies:<br><br>a) The cover letter from the Buyer to Supplier dated TBC<br>b) This Order Form<br>c) The following Annexes in equal order of precedence:<br><br>● Annex 1 - Processing Personal Data<br>● Annex 2 - Specification<br>● Annex 3 - Charges<br>● Annex 4 - Security Schedule |

| Signed for and on behalf of the **Supplier** | Signed for and on behalf of the **Buyer** |
|---|---|
| Name: Redacted Under FOIA Section 40, Personal Information<br><br>Redacted Under FOIA Section 40, Personal Information | Name: Redacted Under FOIA Section 40, Personal Information<br><br>Redacted Under FOIA Section 40, Personal Information |
| Date: | Date: 18/08/2023 |
| Signature: Redacted Under FOIA Section 40, Personal Information | Signature: Redacted Under FOIA Section 40, Personal Information |

# Annex 1 – Authorised Processing Template

| | |
|---|---|
| **Contract:** | Provision of Website Maintenance, Hosting and Development |
| **Date:** | 18/08/2023 |
| **Description Of Authorised Processing** | The Supplier will be authorised under this contract to process personal data of the data subjects, to facilitate their use of the services outlined in annex 2 |
| Subject matter of the processing | Personal Data of data subjects outlined below is used to provide the services described in Annex 2. |
| Duration of the processing | With regards to this contract, the time frame is from 22/04/2023 to the end of the current contract. |
| Nature and purposes of the processing | The nature of the processing will include the storage, organisation, disclosure and destruction of data (by automated and other means) for the purpose of discharging the Inquiry's statutory obligations pursuant to the Inquiries Act 2005 and the Inquiry's Terms of Reference. It will also include the collection, storage, and destruction of contact details, to be directed by the Inquiry. |

| | |
|---|---|
| Type of Personal Data | Personal data – this is typically biographical data such as:<br>• name;<br>• former address details;<br>• still images, voice and video recordings, which includes 999 calls made to the emergency services and closed circuit television.<br><br>In addition, personal data may also include special category data – typically this may include data relating to:<br>• health;<br>• race/ethnicity;<br>• religious beliefs; and<br>• Trade Union membership.<br><br>Some special category data may relate to children. |
| | |
| Categories of Data Subject | Core Participants in the Inquiry, within the meaning of the Inquiries Act 2005:<br>• Other witnesses providing evidence to the Inquiry who are not core participants within the meaning of the Inquiries Act 2005, including Expert Witnesses appointed by the Inquiry; • Members of the Public. |

# [Annex 2 – Specification]

## 1. PURPOSE

**1.1.** The Grenfell Tower Inquiry requires the supplier to continue the support, maintenance and development of its website.

## 2. BACKGROUND TO THE CONTRACTING AUTHORITY

- The Grenfell Tower Inquiry was created to examine the circumstances leading up to and surrounding the fire at Grenfell Tower on the night of 14 June 2017
- The then Prime Minister announced on 15 June 2017 a public Inquiry into the fire at Grenfell Tower on the night of 14 June 2017.
- The Grenfell Tower Inquiry will examine the circumstances leading up to and surrounding the fire.
- Sponsored by the Cabinet Office, this is an independent public Inquiry which requires the hosting of a website to make relevant evidence available to the public.

## 3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

- The Grenfell Tower Inquiry website (https://www.grenfelltowerinquiry.org.uk/) is currently supplied by Digital Craftsmen. As an independent inquiry gov.uk cannot be used so a supplier, Digital Craftsmen Ltd, was sourced through the digital marketplace to build and host a website for the inquiry.

- The current contract is due to end on 21st April 2023 and this paper sets out the need to continue with the current supplier for continuity purposes.

- The website fulfils the inquiry's legal duty as a public Inquiry to make relevant evidence public.
- Therefore, the website therefore holds many thousands of documents and embedded film footage in its evidence section.

- A change in supplier would involve migrating the website and this involves substantial work and a costly process.

- There is a risk of data loss or lack of public access if the supplier is changed.
- The Inquiry has been running for over 5 years and is due to conclude in about 12 months so it is not desirable to have any changes to the look, layout or functionality of the website at this stage.

## 4. DEFINITIONS

| Expression or Acronym | Definition |
|---|---|
| GTI | Grenfell Tower Inquiry |
| TNA | Training Needs Analysis is the process in which the company identifies training and development needs of its employees so they can do their job effectively |

## 5. SCOPE OF REQUIREMENT

**5.1.** The Authority requires the Supplier to continue to deliver website maintenance, hosting and ongoing development for the GTI website.

## 6. THE REQUIREMENT

**6.1.** The Supplier is required to provide:

6.1.1. Website maintenance
6.1.2. App Updates
6.1.3. Hosting
6.1.4. Any ad hoc work as required
6.1.5. Annual penetration test

| | **Managed Support** |
|---|---|
| **Typical Use Cases** | • Production |
| **Support Hours** | • 24x7 critical support |
| **Service desk SLA** | • 95% |
| **Management Procedures** | • ISO 27001 accredited management system<br>• Capacity reporting<br>• Change Management |
| **Email** | • SMTP managed delivery |
| **Monitoring** | • Advanced Monitoring (basic monitoring and key service metrics) • Triaged alerts |
| **Troubleshooting** | • Incident reporting |
| **Security** | • Secure VPN<br>• Operating system patching<br>• Managed Firewall |
| **Configuration** | • Set up<br>• Configuration help<br>• Configuration Management |

| | |
|---|---|
| **Domain Management** | • Domain registration<br>• SSL certificates<br>• DNS management |
| **Backup** | •Daily backup<br>• Backup testing |
| **Migration** | • Upgrades<br>• Consolidation |

## 7. KEY MILESTONES AND DELIVERABLES

**7.1.** The following Contract milestones/deliverables shall apply:

| Milestone/Deliverable | Description | Timeframe or Delivery Date |
|---|---|---|
| 1 | Increase functionality as need grows | In response to increased demand |
| 2 | Maintain security of personal information stored on site | Throughout the course of the contract |
| 3 | Ensure site remains operational, and can be archived by TNA to remain operational after closure of the Inquiry | Through the course of the contract |
| 4 | Supplier to work closely with Buyer and Cabinet Office to ensure users' accessibility needs are met | As required |

## 8. MANAGEMENT INFORMATION/REPORTING

**8.1.** Quarterly management meetings to update on performance, development progress and finance.

## 9. VOLUMES

**9.1.** N/A

## 10. CONTINUOUS IMPROVEMENT

**10.1.** The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

**10.2.** The Supplier should present new ways of working to the Authority during quarterly Contract review meetings.

**10.3.** Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

## 11. SUSTAINABILITY

**11.1.** The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the project duration.

**11.2.** Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

## 12. QUALITY

**12.1.** Suppliers should note the UK Government Service Standards can be referenced on this site: https://www.gov.uk/service-manual/service-standard

**12.2.** The Supplier shall demonstrate how their proposed technical solution will ensure the ability to incorporate and meet WCAG 2.1 AA Accessibility Standards if developed fully.

## 13. PRICE

**13.1.** The maximum budget available for this requirement, excluding optional support services post 28 April 2023, is £38,556 excluding VAT excluding VAT.

Any proposal submitted above this value will be deemed non-compliant and excluded from the competition.

# 14. STAFF AND CUSTOMER SERVICE

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

**14.2.** The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

**14.3.** The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

**14.4.** The Supplier Staff will:

14.4.1. Fulfil all reasonable requests of the Buyer;

14.4.2. Apply all due skill, care and diligence to the provisions of the Services;

14.4.3. Be appropriately experienced, qualified and trained to supply the Services;

14.4.4. Respond to any enquiries about the Services as soon as reasonably possible;

14.4.5. Complete any necessary vetting procedures specified by the Buyer.

## 15. SERVICE LEVELS AND PERFORMANCE

**15.1.** The Authority will measure the quality of the Supplier's delivery by:

| KPI/SLA | Service Area | KPI/SLA description | Target |
|---|---|---|---|
| 1 | Website disruption | If website is inaccessible or non-functional for majority of users | 1 hour response and 2 hour resolution |
| 2 | Website disruption | If the website is inaccessible or partially non-functional for a portion of users. Suitable workaround available | 1 hour response and 4 hour resolution |
| 3 | Website disruption | If the website is partially inaccessible or non-functional for a portion of users. | 1 hour response and 16 hour resolution |

| Categories Of Incidents | Illustrative Description | Normal Response Time | Response time target |
|---|---|---|---|
| Critical | ● Breach of security<br>● Site becomes unavailable/unusable<br>● Urgent content removal is required. | 30 Mins | 1 Hour |
| Severe | ● Site becomes significantly compromised (for | 1 Hour | 3 Hours |
| | instance, total search failure);<br>● Infrastructure failure that leads to reliance on one point of failure;<br>● Urgent content changes are required that can not be completed through the CMS due to internal staff being unavailable. | | |

| | | | |
|---|---|---|---|
| Minor | • Minor site issues;<br>• Performance slowdowns and<br>• cosmetic issues; CSS issues. | 3 Hours | 24 Hours |

## 16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

**16.1.** ISO 27001 – Information Security Controls

**16.2.** Cyber- Essentials Plus Certification

**16.3.** Supplier staff to sign Buyer's confidentiality undertaking

## 17. PAYMENT AND INVOICING

**17.1.** Payment will be made in line with the proportion of work completed, for work undertaken and received to the end of this current financial year, where a deliverable may not necessarily be completed.

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

**17.3.** Invoices should be submitted to: apinvoices-cab-u@gov.sscl copying in finance@grenfelltowerinquiry.org.uk.

**17.4.** It is a requirement that a PO number should always be quoted on the invoice to ensure prompt payment.

## 18. CONTRACT MANAGEMENT

**18.1.** Contract Management shall be carried out in accordance with the Key Milestones and SLAs set out in this Statement of Requirements.

**18.2.** Attendance at Contract Review meetings shall be at the Supplier's own expense.

## 19. LOCATION

**19.1.** Office space will not be provided. Where in-person meetings are requested or required by the Authority, these will be at Grenfell Tower Inquiry Team, 1st Floor, 1 Giltspur St, London, EC1A 9DD , unless the Authority agrees to an alternative location.

**19.2.** The location of the Services will be carried out at the Supplier's premises.

# [Annex 3 – Charges]

The Charges for the deliverables shall not exceed £38,556 + VAT

# [Annex 4 – Security Schedule ]

## 1 Buyer Options

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:

| | | |
|---|---|---|
| **Buyer risk assessment** (see Paragraph 2) | | |
| The Buyer has assessed this Agreement as: | a higher-risk agreement | ☐ |
| | a standard agreement | ☒ |
| **Certifications** (see Paragraph 8) (applicable only for standard risk agreements) | | |
| Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must have the following Certifications: | Cyber Essentials Plus | ☒ |
| | Cyber Essentials | ☐ |
| **Locations** (see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Sub-contractors 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 | ☐ |
| **Support Locations** (see Paragraph 1 of the Security Requirements) | | |
| The Supplier and Subcontractors may operate Support Locations in: | the United Kingdom only | ☒ |
| | the United Kingdom and European Economic Area only | ☒ |
| | anywhere in the world not prohibited by the Buyer | ☐ |

## 2 Buyer risk assessment

2.1 Where the Buyer has assessed this Agreement as a higher-risk agreement, the Supplier must: (a) comply with all requirements of this Schedule [♦] (*Security Management*); and

(b) hold the ISO/IEC 27001:2013 Relevant Certification from a UKAS-approved certification body (see Paragraph 8).



2.2 Where the Buyer has assessed this Agreement as a standard risk agreement, the Supplier must comply with all requirements of this this Schedule [♦] (*Security Management*) except:

(a) Paragraph 9 (*Security Management Plan*);

(b) paragraph 9 of the Security Requirements (*Code Reviews*);

(c) paragraph 11 of the Security Requirements (*Third-party Software Modules*);

(d) paragraph 12 of the Security Requirements (*Hardware and software support*); (e) paragraph 13 of the Security Requirements (*Encryption*); and

(f) paragraph 19 of the Security Requirements (*Access Control*).

2.3 Where the Buyer has not made an assessment in the table in Paragraph 1, the Parties must treat this Agreement as a higher-risk agreement.

## 3 Definitions

3.1 In this Schedule [ ♦] (*Security Management*):

| | |
|---|---|
| **"Anti-virus Software"** | means software that:<br>(a) protects the Supplier Information Management System from the possible introduction of Malicious Software;<br>(b) scans for and identifies possible Malicious Software in the Supplier Information Management System;<br>(c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:<br>(i) prevents the harmful effects of the Malicious Software; and<br>(ii) removes the Malicious Software from the Supplier Information Management System; |
| **"Breach Action Plan"** | means a plan prepared under paragraph 22.3 of the Security Requirements addressing any Breach of Security; |
| **"Breach of Security"** | means the occurrence of: |



| | |
|---|---|
| | (a) any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement, including the Buyer Data and the Code;<br>(d) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Subcontractor in connection with this Agreement, including the Buyer Data and the Code; and/or<br>(e) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; (f) the installation of Malicious Software in the:<br>(i) Supplier Information Management System;<br>(ii) Development Environment; or<br>(iii) Developed System; |

| | |
|---|---|
| | (g) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the:<br>(i) Supplier Information Management System;<br>(ii) Development Environment; or<br>(iii) Developed System; and<br>(h) includes any attempt to undertake the activities listed in subparagraph (a) where the Supplier has reasonable grounds to suspect that attempt:<br>(i) was part of a wider effort to access information and communications technology by or on behalf of Central Government Bodies; or<br>(ii) was undertaken, or directed by, a state other than the United Kingdom |
| **"Buyer Data"** | means any:<br>(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;<br>(b) Personal Data for which the Buyer is a, or the, Data Controller; or<br>(c) any meta-data relating to categories of data referred to in paragraphs (a) or (b);<br>that is: (a) supplied to the Supplier by or on behalf of the Buyer; or<br>(b) 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. |
| **"Buyer Data Register"** | means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with paragraph 23 of the Security Requirements; |
| **"Buyer Equipment"** | means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System; |

| | |
|---|---|
| **"Buyer System"** | means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services; |
| **"Certification Default"** | means the occurrence of one or more of the circumstances listed in Paragraph 8.4; |
| **"Certification Rectification Plan"** | means the plan referred to in Paragraph 8.5(a); |
| **"Certification Requirements"** | means the requirements set out in paragraph 8.3. |
| **"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:<br>(a) has been certified by the National Cyber Security Centre;<br>(b) holds "Green Light" status; and<br>(c) is authorised to provide the IT Health Check services required by paragraph 18 of the Security Requirements; |
| **"Code"** | means, in respect of the Developed System:<br>(a) the source code; (b) the object code;<br>(c) third-party components, including third-party coding frameworks and libraries; and (d) all supporting documentation. |

| | |
|---|---|
| **"Code Review"** | means a periodic review of the Code by manual or automated means to: (a) identify and fix any bugs; and (b) ensure the Code complies with: (i) the requirements of this Schedule [♦] (*Security Management*); and (ii) the Secure Development Guidance; |
| **"Code Review Plan"** | means the document agreed with the Buyer under paragraph 9.3 of the Security Requirements setting out the requirements for, and frequency of, Code Reviews; |



| | |
|---|---|
| **"Code Review Report"** | means a report setting out the findings of a Code Review; |
| **"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 National Cyber Security Centre; |
| **"Developed System"** | means the software or system that the Supplier will develop under this Agreement; |
| **"Development Activity"** | means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (c) code storage; and (d) deployment. |

| | |
|---|---|
| **"Development Environment"** | means any information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Development Activity; |
| **"EEA"** | means the European Economic Area; |
| **"End-user Device"** | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services. |
| **"Email Service"** | means a service that will send, or can be used to send, emails from the Buyer's email address or otherwise on behalf of the Buyer; |
| "**HMG Baseline Personnel Security Standard**" | means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 (https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/714002/ HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time; |
| "**IT Health Check**" | means security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment in accordance with paragraph 33 of the Security Requirements; |
| "**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; |
| "**Modules Register**" | means the register of Third-party Software Modules required for higher risk agreements by paragraph 11.3 of the Security Requirements; |



| | |
|---|---|
| "**NCSC**" | means the National Cyber Security Centre; |

| | |
|---|---|
| "**NCSC 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-thecloud-security-principles. |
| "**NCSC Device Guidance**" | means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance; |
| "**NCSC Protecting Bulk Personal Data Guidance**" | means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data |
| "**NCSC Secure Design Principles"** | means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles. |
| "**OWASP**" | means the Open Web Application Security Project Foundation; |
| "**OWASP Secure Coding Practice**" | means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference guide/migrated_content; |
| "**OWASP Top Ten**" | means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www project-top-ten/; |
| "**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; |
| "**Prohibited Activity**" | means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice; |
| "**Prohibition Notice**" | means a notice issued under paragraph 1.8 of the Security Requirements. |
| "**Protective Monitoring System**" | means the system implemented by the Supplier and its Sub-contractors under paragraph 20.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code |
| "**Register of Support Locations and Third-Party Tools**" | means the part of the Security Management Plan setting out, in respect of Support Locations and Third-Party Tools:<br>(a) the nature of the activity performed at the Support Location or by the Third-Party Tool on the Code or the Buyer Data (as applicable);<br>(b) where that activity is performed by individuals, the place or facility from where that activity is performed; and |



| | |
|---|---|
| | (c) in respect of the entity providing the Support Locations or Third-Party Tools, its:<br>(i) full legal name;<br>(ii) trading name (if any)<br>(iii) country of registration;<br>(iv) registration number (if applicable); and (v) registered address. |
| "**Relevant Activities**" | means those activities specified in paragraph 0 of the Security Requirements. |

| | |
|---|---|
| "**Relevant Certifications**" | means<br>(a) in the case of a standard agreement:<br>(i) Cyber Essentials; and/or (ii) Cyber Essentials Plus as determined by the Buyer; or<br>(b) in the case of a higher risk agreement:<br>(i) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and<br>(ii) Cyber Essentials Plus; |
| "**Relevant Convictions**" | means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify |
| "**Remediation Action Plan**" | means the plan prepared by the Supplier in accordance with Paragraph 18.11 to 18.15, addressing the vulnerabilities and findings in a IT Health Check report |
| "**Secure Development Guidance**" | means:<br>(a) the NCSC's document "Secure development and deployment guidance" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/developers-collection; and<br>(b) the OWASP Secure Coding Practice as updated or replaced from time to time; |
| "**Security Management Plan**" | means the document prepared in accordance with the requirements of Paragraph 9 and in the format, and containing the information, specified in Annex 2. |
| "**SMP Sub contractor**" | means a Sub-contractor with significant market power, such that: |

| | |
|---|---|
| | (a) they will not contract other than on their own contractual terms; and (b) either:<br>(i) there are no other substitutable suppliers of the particular services other than SMP Sub contractors; or<br>(ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services. |
| "**Sites**" | means any premises:<br>(a) from or at which:<br>(i) the Services are (or are to be) provided; or<br>(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where:<br>(i) any part of the Supplier Information Management System is situated; or<br>(ii) any physical interface with the Buyer System takes place; and<br>(c) for the avoidance of doubt include any premises at which Development Activities take place |
| "**Sub-contractor**" | includes, for the purposes of this Schedule [♦] (*Security Management*), any individual or entity that:<br>(a) forms part of the supply chain of the Supplier; and<br>(b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data; |
| "**Sub-contractor Personnel**" | means:<br>(a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and<br>(b) engaged in or likely to be engaged in:<br>(i) the performance or management of the Services;<br>(ii) or the provision of facilities or services that are necessary for the provision of the Services. |

| | |
|---|---|
| "**Supplier Information Management System**" | means:<br>(a) those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services;<br>(b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and<br>(c) for the avoidance of doubt includes the Development Environment. |



| | |
|---|---|
| "**Security Requirements**" | mean the security requirements in Annex 1 to this Schedule [♦] (*Security Management*) |
| "**Supplier Personnel**" | means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier's obligations under this Agreement; |
| "**Support Location**" | means a place or facility where or from which individuals may access or Process the Code or the Buyer Data; |
| "**Support Register**" | means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Agreements in accordance with paragraph 12 of the Security Requirements. |
| "**Third-party Software Module**" | means any module, library or framework that:<br>(a) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and (b) either:<br>(i) forms, or will form, part of the Code; or<br>(ii) is, or will be, accessed by the Developed System during its operation. |
| "**Third-party Tool**" | means any activity conducted other than by the Supplier during which the Code or the Buyer Data is accessed, analysed or modified or some form of operation is performed on it; |
| "**UKAS**" | means the United Kingdom Accreditation Service; |

## 4 Introduction

4.1 This Schedule [♦] (*Security Management*) sets out:

(a) the assessment of this Agreement as either a:

(i) higher risk agreement; or (ii) standard agreement, in Paragraph 1;

(b) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of:

(i) the Development Activity;

(ii) the Development Environment;

(iii) the Buyer Data;

(iv) the Services; and

(v) the Supplier Information Management System;



(c) the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;

(d) the Buyer's access to the Supplier Personnel and Supplier Information

Management System, in Paragraph 7;

(e) the Certification Requirements, in Paragraph 8;

(f) the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 9; and

(g) the Security Requirements with which the Supplier and its Sub-contractors must comply.

## 5 Principles of Security

5.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data, and the integrity and availability of the Developed System, and, consequently, on the security of:

(a) the Sites;

(b) the Services; and

(c) the Supplier's Information Management System.

5.2 The Parties shall share information and act in a co-operative manner at all times to further the principles of security in Paragraph 5.1.

5.3 Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:

(a) the security, confidentiality, integrity and availability of the Buyer Data when that Buyer

Data is under the control of the Supplier or any of its Sub-contractors;

(b) the security and integrity of the Developed System; and

(c) the security of the Supplier Information Management System.

5.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

## 6 Security Requirements

6.1 The Supplier shall:

(a) comply with the Security Requirements; and

(b) subject to Paragraph 6.2, ensure that all Sub-contractors also comply with the Security Requirements.

6.2 Where a Sub-contractor is SMP Sub-contractor, the Supplier shall:

(a) use best endeavours to ensure that the SMP Sub-contractor complies with the Security Requirements;



(b) document the differences between Security Requirements the obligations that the SMP Sub contractor is prepared to accept in sufficient detail to allow the Buyer to form an informed view of the risks concerned;

(c) take such steps as the Buyer may require to mitigate those risks.

## 7 Access to Supplier Personnel and Supplier Information Management System

7.1 The Buyer may require, and the Supplier must provide, and ensure that each Subcontractor provides, the Buyer and its authorised representatives with:

(a) access to the Supplier Personnel, including, for the avoidance of doubt, the Subcontractor Personnel;

(b) access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Sub contractor; and

(c) such other information and/or documentation that the Buyer or its authorised representatives may require, to allow the Buyer to audit the Supplier and its Sub-contractors' compliance with this Schedule [◆] (*Security Management*) and the Security Requirements.

7.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 7.1: (a) in the case of a Breach of Security within 24 hours of such a request; and (b) in all other cases, within 10 Working Days of such request.

## 8 Certification Requirements

8.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer,

both: (a) it; and

(b) any Sub-contractor, is certified as compliant with the

Relevant Certifications.

8.2 Unless otherwise agreed by the Buyer, before it begins to provide the Services, the Supplier must provide the Buyer with a copy of:

(a) the Relevant Certifications for it and any Sub-contractor; and

(b) in the case of a higher-risk agreement, any relevant scope and statement of applicability required under the ISO/IEC 27001:2013 Relevant Certifications.

8.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications for it and any Sub-contractor are:

(a) currently in effect;

(b) cover at least the full scope of the Supplier Information Management System; and

(c) are not subject to any condition that may impact the provision of the Services or the Development Activity (the "**Certification Requirements**").



8.4 The Supplier must notify the Buyer promptly, and in any event within three (3) Working Days,

after becoming aware that, in respect of it or any Sub-contractor: (a) a Relevant

Certification has been revoked or cancelled by the body that awarded it; (b) a Relevant

Certification expired and has not been renewed by the Supplier;

(c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System; or

(d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a "**Certification Default**")

8.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 8.4:

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 8.4 (or such other period as the Parties may agree) provide a draft plan (a "**Certification Rectification Plan**") to the Buyer setting out:

(i) full details of the Certification Default, including a root cause analysis;

(ii) the actual and anticipated effects of the Certification Default;

(iii) the steps the Supplier and any Sub-contractor to which the Certification Default relates will take to remedy the Certification Default;

(b) the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

(c) if the Buyer rejects the Certification Rectification Plan, the Supplier must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph (b) will apply to the re-submitted plan;

(d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

(e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

## 9 Security Management Plan

9.1 This Paragraph 9 applies only where the Buyer has assessed that this Agreement is a higherrisk agreement.

*Preparation of Security Management Plan*

9.2 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 Development Environment, the Developed System, the Buyer Data and the Supplier Information Management System.

9.3 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) an assessment of the Supplier Information Management System against the requirements of this Schedule [♦] (*Security Management*), including the Security Requirements;



(b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System. the Buyer Data, the Buyer, the Services and/or users of the Services; and

(c) the following information, so far as is applicable, in respect of each

Sub-contractor: (i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any);

(C) registration details (where the Sub-contractor is not an individual);

(ii) the Relevant Certifications held by the Sub-contractor;

(iii) the Sites used by the Sub-contractor;

(iv) the Development Activity undertaken by the Sub-contractor;

(v) the access the Sub-contractor has to the Development

Environment; (vi) the Buyer Data Processed by the Sub-contractor;

(vii) the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

(viii) the measures the Sub-contractor has in place to comply with the requirements of this Schedule [♦] (*Security Management*);

(d) the Register of Support Locations and Third Party Tools;

(e) the Modules Register;

(f) the Support Register;

(g) details of the steps taken to comply with:

(i) the Secure Development Guidance; and

(ii) the secure development policy required by the ISO/IEC 27001:2013 Relevant Certifications;

(h) details of the protective monitoring that the Supplier will undertake in accordance with paragraph 20 of the Security Requirements, including:

(i) the additional audit and monitoring the Supplier will undertake of the Supplier Information Management System and the Development environment; and

(ii) the retention periods for audit records and event logs.

 *Approval of Security Management Plan*

9.4 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 use the Supplier Information Management System to:

(i) undertake the Development Activity; and/or

(ii) Process Buyer Data; or

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

9.5 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.

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

*Updating Security Management Plan*

9.7 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*

9.8 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.

9.9 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.



# Annex 1 Security Requirements

## 1 Location

*Location for Relevant Activities*

The Short form Contract

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and ensure that its Sub-contractors, at all times:

(a) undertake the Development Activity;

(b) host the Development Environment; and

(c) store, access or process Buyer Data,

(the "**Relevant Activities**") only in the geographic areas permitted by the Buyer.

1.2 Where the Buyer has permitted the Supplier and its Sub-contractors to perform the Relevant Activities outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors undertake the Relevant Activities in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (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 Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Buyer with such information as the Buyer requires

concerning: (i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.8. 1.3

Where the Supplier cannot comply with one or more of the requirements of paragraph 1.2: (a) it

must provide the Buyer with such information as the Buyer requests concerning: (i)

the security controls in places at the relevant location or locations; and

(ii) where certain security controls are not, or only partially, implemented the reasons for this;

(b) the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and

(c) if the Buyer does not grant permission to use that location or those locations, the Supplier must, within such period as the Buyer may specify:

(i) cease to store, access or process Buyer Data at that location or those locations;



(ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or

process Buyer Data at that location, or those locations, as the Buyer may specify.

*Support Locations*

1.4 The Supplier must ensure that all Support Locations are located only in the geographic areas permitted by the Buyer.

1.5 Where the Buyer has permitted the Supplier and its Sub-contractors to operate Support Locations outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Sub-contractors operate the Support Locations in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Sub-contractor (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 Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;

(d) the Supplier has provided the Authority with such information as the Authority requires concerning:

(i) the entity;

(ii) the arrangements with the entity; and

(iii) the entity's compliance with the binding agreement; and

(e) the Authority has not given the Supplier notice under paragraph 1.8.

*Third-party Tools*

1.6 The Supplier must use, and ensure that Sub-contractors use, only those Third-party Tools included in the Register of Support Locations and Third-party Tools.

1.7 The Supplier must not, and must not allow Sub-contractors to, use a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer.

*Prohibited Activities*

1.8 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub contractors must not undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a "**Prohibited Activity**").

(a) in any particular country or group of countries;

(b) in or using facilities operated by any particular entity or group of entities; or

(c) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity,

(a "**Prohibition Notice**").

1.9 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Prohibited Activities affected by the notice, the Supplier must, and must procure that Sub-



contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

## 2 Vetting, Training and Staff Access

*Vetting before performing or managing Services*

2.1 The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:

(a) Development Activity;

(b) any activity that provides access to the Development Environment; or (c) any activity

relating to the performance and management of the Services unless:

(d) that individual has passed the security checks listed in paragraph 2.2; or

(e) the Buyer has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, the security checks are:

(a) the checks required for the HMG Baseline Personnel Security Standard (BPSS) to

verify: (i) the individual's identity;

(ii) the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

(iii) the individual's previous employment history; and

(iv) that the individual has no Relevant Convictions;

(b) national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

(c) such other checks for the Supplier Personnel of Sub-contractors as the Buyer may

specify. *Annual training*

2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:

(a) General training concerning security and data handling; and

(b) Phishing, including the dangers from ransomware and other malware.

*Staff access*

2.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to



the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Subcontractors remove, an individual Supplier Personnel's access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

*Exception for certain Sub-contractors*

2.7 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Personnel will perform as the Buyer reasonably requires; and

(c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Subcontractor.

## 3 End-user Devices

3.1 The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data or Code is stored or processed in accordance with the following requirements:

(a) the operating system and any applications that store, process or have access to Buyer Data or Code 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 Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;

(d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of

technical policies and controls over applications that have access to Buyer Data and Code to ensure the security of that Buyer Data and Code;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the Enduser Device, remove or make inaccessible all Buyer Data or Code 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 Relevant Certification.

3.2 The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

3.3 Where there is any conflict between the requirements of this Schedule [◆] (*Security Management*) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.



## 4 Secure Architecture

4.1 The Supplier shall design and build the Developed System in a manner consistent with:

(a) the NCSC's guidance on "Security Design Principles for Digital Services";

(b) where the Developed System will Process bulk data, the NCSC's guidance on "Bulk Data Principles"; and

(c) the NCSC's guidance on "Cloud Security Principles".

4.2 Where any of the documents referred to in paragraph 4.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

## 5 Secure Software Development by Design

5.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, implement secure development and deployment practices to ensure that:

(a) no malicious code is introduced into the Developed System or the Supplier Information Management System.

(b) the Developed System can continue to function in accordance with the

Specification: (i) in unforeseen circumstances; and

(ii) notwithstanding any attack on the Developed System using common cyberattack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

5.2 To those ends, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

(a) comply with the Secure Development Guidance as if its requirements were terms of this Contract; and

(b) document the steps taken to comply with that guidance as part of the Security Management Plan.

5.3 In particular, the Supplier must, and ensure that all Sub-contractors engaged in Development Activity:

(a) ensure that all Supplier Staff engaged in Development Activity are:

(i) trained and experienced in secure by design code development;

(ii) provided with regular training in secure software development

and deployment; (b) ensure that all Code:

(i) is subject to a clear, well-organised, logical and documented architecture;

(ii) follows OWASP Secure Coding Practice

(iii) follows recognised secure coding standard, where one is available;

(iv) employs consistent naming conventions;



(v) is coded in a consistent manner and style;

(vi) is clearly and adequately documented to set out the function of each section of code;

(vii) is subject to appropriate levels of review through automated and nonautomated methods both as part of: (A) any original coding; and (B) at any time the Code is changed;

(c) ensure that all Development Environments:

(i) protect access credentials and secret keys;

(ii) are logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;

(iii) require multi-factor authentication to access;

(iv) have onward technical controls to protect the Developed System or the Supplier Information Management System in the event a Development Environment is compromised;

(v) use network architecture controls to constrain access from the Development Environment to the Developed System or the Supplier Information Management System;

## 6 Code Repository and Deployment Pipeline

7 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity:

7.1 when using a cloud-based code depository for the deployment pipeline, use only a cloudbased code depository that has been assessed against the NCSC Cloud Security Principles;

7.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;

7.3 ensure secret credentials are separated from source code.

7.4 run automatic security testing as part of any deployment of the Developed System.

## 8 Development and Testing Data

8.1 The Supplier must, and must ensure that all Sub-contractors engaged in Development Activity, use only anonymised, dummy or synthetic data when using data within the Development Environment for the purposes of development and testing, .

## 9 Code Reviews

9.1 This paragraph applies where the Buyer has assessed that this Agreement is a higherrisk agreement.

9.2 The Supplier must:

(a) regularly; or



(b) as required by the Buyer review the Code in accordance with the requirements of this paragraph 9 (a "**Code Review**"). 9.3 Before conducting any Code Review, the Supplier must agree with the Buyer:

(a) the modules or elements of the Code subject to the Code Review;

(b) the development state at which the Code Review will take place;

(c) any specific security vulnerabilities the Code Review will assess; and (d) the frequency of any Code Reviews (the "**Code Review Plan**").

9.4 For the avoidance of doubt, the Code Review Plan may specify different modules or elements of the Code are reviewed at a different development state, for different security vulnerabilities and at different frequencies.

9.5 The Supplier:

(a) must undertake Code Reviews in accordance with the Code Review Plan; and

(b) may undertake Code Reviews by automated means if this is consistent with the approach specified in the Code review Plan.

9.6 No later than 10 Working Days or each Code Review, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the Code Review Report.

9.7 Where the Code Review identifies any security vulnerabilities, the Supplier must: (a)

remedy these at its own cost and expense;

(b) ensure, so far as reasonably practicable, that the identified security vulnerabilities are not present in any other modules or code elements; and

(c) modify its approach to undertaking the Development Activities to ensure, so far as is practicable, the identified security vulnerabilities will not re-occur; and

(d) provide the Buyer with such information as it requests about the steps the Supplier takes under this paragraph 9.7.

## 10 Third-party Software

10.1 The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Process the Buyer Data greater than those rights strictly necessary for the use of the software.

## 11 Third-party Software Modules

11.1 This paragraph 11 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement

11.2 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:

(a) verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;



(b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;

(c) continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;

(d) take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.

11.3 The Supplier must produce and maintain a register of all Third-party Software Modules that form part of the Code (the "**Modules Register**").

11.4 The Modules Register must include, in respect of each Third-party Software

Module: (a) full details of the developer of the module;

(b) the due diligence the Supplier undertook on the Third-party Software Module before deciding to use it;

(c) any recognised security vulnerabilities in the Third-party Software Module; and

(d) how the Supplier will minimise the effect of any such security vulnerability on the Developed System.

11.5 The Supplier must:

(a) review and update the Modules Register:

(i) within 10 Working Days of becoming aware of a security vulnerability in any Third party Software Module; and

(ii) at least once every 6 (six) months;

(b) provide the Buyer with a copy of the Modules Register: (i) whenever it updates

the Modules Register; and (ii) otherwise when the Buyer requests.

## 12 Hardware and software support

12.1 This paragraph 12 applies only where the Buyer has assessed that this Agreement is a higher-risk agreement

12.2 The Supplier must ensure that all software used to provide the Services remains at all times in full security support, including any extended or bespoke security support.

12.3 The Supplier must produce and maintain a register of all software that form the Supplier Information Management System (the "**Support Register**").

12.4 The Support Register must include in respect of each item of software:

(a) the date, so far as it is known, that the item will cease to be in mainstream security

support; and

(b) the Supplier's plans to upgrade the item before it ceases to be in mainstream security support.



12.5 The Supplier must:

(a) review and update the Support Register:

(i) within 10 Working Days of becoming aware of the date on which, or any change to the date on which, any item of software will cease to be in mainstream security report;

(ii) within 10 Working Days of introducing new software, or removing existing software, from the Supplier Information Management System; and

(iii) at least once every 12 (twelve) months;

(b) provide the Buyer with a copy of the Support Register: (i) whenever it updates the Support Register; and

(ii) otherwise when the Buyer requests.

12.6 Where any element of the Developed System consists of COTS Software, the Supplier shall ensure:

(a) those elements are always in mainstream or extended security support from the relevant vendor; and

(b) the COTS Software is not more than one version or major release behind the latest version of the software.

12.7 The Supplier shall ensure that all hardware used to provide the Services, whether used by the Supplier or any Sub-contractor is, at all times, remains in mainstream vendor support, that is, that in respect of the hardware, the vendor continues to provide:

(a) regular firmware updates to the hardware; and

(b) a physical repair or replacement service for the hardware.

## 13 Encryption

13.1 This paragraph applies where the Buyer has assessed that this Agreement is a higherrisk agreement.

13.2 Before Processing any Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Process Buyer Data will use to comply with this paragraph 13.

13.3 Where this paragraph 13 requires Buyer Data to be encrypted, the Supplier must use, and ensure that Subcontractors use, the methods agreed by the Buyer under paragraph 13.2.

13.4 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that the Developed System encrypts Buyer Data: (a) when the Buyer Data is stored at any time when no operation is being performed on it; and (b) when the buyer Data is transmitted.

13.5 Unless paragraph 13.6 applies, the Supplier must ensure, and must ensure that all Subcontractors ensure, that Buyer Data is encrypted:

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



when transmitted.

13.6 Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 13.5, the Supplier must:

(a) immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;

(c) provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.

13.7 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.

13.8 Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

(a) the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;

(b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.

13.9 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].

## 14 Email

14.1 Notwithstanding anything in the specification for the Developed System or this Agreement, the Supplier must ensure that where the Developed System will provide an Email Service to the Buyer, the Developed System:

(a) supports transport layer security ("**TLS**") version 1.2, or higher, for sending and receiving emails;

(b) supports TLS Reporting ("**TLS-RPT**"); (c) is capable of

implementing:

(i) domain-based message authentication, reporting and conformance

("**DMARC**"); (ii) sender policy framework ("**SPF**"); and

(iii) domain keys identified mail ("**DKIM**"); and

(d) is capable of complying in all respects with any guidance concerning email security as issued or updated from time to time by:

(i) the UK Government (current version at https://www.gov.uk/guidance/set-up government-email-services-securely; or

(ii) the NCSC (current version at https://www.ncsc.gov.uk/collection/emailsecurity- and anti-spoofing).

## 15 DNS

15.1 Unless otherwise agreed by the Buyer, the Supplier must ensure that the Developed System uses the UK public sector Protective DNS ("**PDNS**") service to resolve internet DNS queries.

## 16 Malicious Software

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

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

(a) prevents the installation of the most common forms of Malicious Software in the Supplier Information Management System and the Development Environment;

(b) is configured to perform automatic software and definition updates;

(c) provides for all updates to be the Anti-virus Software to be deployed within 10 Working Days of the update's release by the vendor;

(d) performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and

(e) where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

16.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any [Losses] and to restore the Services to their desired operating efficiency.

16.4 The Supplier must at all times, during and after the [Term], on written demand indemnify the Buyer and keep the Buyer indemnified, against all [Losses] incurred by, awarded against or agreed to be paid by the Buyer arising from any Breach of Security caused by Malicious Software where the Breach of Security arose from a failure by the Supplier, or a Subcontractor, to comply with this paragraph .

## 17 Vulnerabilities

17.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Subcontractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:

(a) seven (7) days after the public release of patches for vulnerabilities classified as "critical";

(b) thirty (30) days after the public release of patches for vulnerabilities classified as "important"; and

(c) sixty (60) days after the public release of patches for vulnerabilities classified as

"other". 17.2 The Supplier must:

(a) scan the Supplier Information Management System and the Development Environment 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 17.1.



17.3 For the purposes of this paragraph 17, the Supplier must implement a method for classifying vulnerabilities to the Supplier Information Management System as “critical”, “important” or “other” that is aligned to recognised vulnerability assessment systems, such as:

(a) the National Vulnerability Database’s vulnerability security ratings; or (b)

Microsoft’s security bulletin severity rating system.

## 18 Security testing

*Responsibility for security testing*

18.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 18 (unless the Buyer gives notice under Paragraph 18.2); and

(b) the costs of implementing any findings, or remedying any vulnerabilities, identified in that security testing.

*Security tests by Buyer*

18.2 The Supplier may give notice to the Supplier that the Buyer will undertake the security testing required by Paragraph 18.4(a) and 18.4(d).

18.3 Where the Buyer gives notice under Paragraph 18.2:

(a) the Supplier shall provide such reasonable co-operation as the Buyer requests, including:

(i) such access to the Supplier Information Management System as the Buyer may request; and

(ii) such technical and other information relating to the Information Management System as the Buyer requests;

(b) the Buyer must provide a full, unedited and unredacted copy of the report relating to the IT Health Check as soon as reasonably practicable after the Buyer receives a copy of the report; and

(c) for the purposes of Paragraphs 18.8 to 18.17:

(i) the Supplier must treat any IT Health Check commissioned by the Buyer as if it were such a report commissioned by the Supplier; and

(ii) the time limits in Paragraphs 18.8 and 18.11 run from the date on which the Buyer provides the Supplier with the copy of the report under Paragraph (b). *Security tests by Supplier*

18.4 The Supplier must:

(a) during the testing of the Developed System and before the Developed System goes live (unless the Buyer gives notice under Paragraph 18.2);

(b) at least once during each [Contract Year]; and (c) when required to do so by

the Buyer; undertake the following activities:



(d) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an "**IT Health Check**") in accordance with Paragraph 18.5 to 18.7; and

(e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 18.8 to 18.17.

*IT Health Checks*

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

(a) use only a CHECK 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 Information Management System and the delivery of the Services.

(c) promptly provide the Buyer with such technical and other information relating to the

Information Management System as the Buyer requests; (d) include within the scope

of the IT Health Check such tests as the Buyer requires; (e) agree with the Buyer the

scope, aim and timing of the IT Health Check.

18.6 The Supplier must commission the IT Health Check in accordance with the scope, aim and timing agreed by the Buyer.

18.7 Following completion of an IT Health Check, the Supplier must provide the Buyer with a full, unedited and unredacted copy of the report relating to the IT Health Check without delay and in any event within 10 Working Days of its receipt by the Supplier.

*Remedying vulnerabilities*

18.8 In addition to complying with Paragraphs 18.4 to 18.17, the Supplier must remedy:

(a) any vulnerabilities classified as critical in the IT Health Check report within 5 Working Days of becoming aware of the vulnerability and its classification;

(b) any vulnerabilities classified as high in the IT Health Check report within 1 month of becoming aware of the vulnerability and its classification; and

(c) any vulnerabilities classified as medium in the IT Health Check report within 3 months of becoming aware of the vulnerability and its classification.

18.9 The Supplier must notify the Buyer immediately if it does not, or considers it will not be able to, remedy the vulnerabilities classified as critical, high or medium in the IT Health Check report within the time periods specified in Paragraph 18.8.

*Significant vulnerabilities*

18.10 Where the IT Health Check report identifies more than 10 vulnerabilities classified as either critical or high, the Buyer may, at the Supplier's cost, appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities.

*Responding to an IT Health Check report*

18.11 Where the IT Health Check identifies vulnerabilities in, or makes findings in respect of, the Information Management System, the Supplier must within 20 Working Days of receiving the IT



Health Check report, prepare and submit for approval to the Buyer a draft plan addressing the vulnerabilities and findings (the "**Remediation Action Plan**").

18.12 Where the Buyer has commissioned a root cause analysis under Paragraph 18.10, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

18.13 The draft Remediation Action Plan must, in respect of each vulnerability identified or finding made by the IT Health Check report:

(a) how the vulnerability or finding will be remedied;

(b) the date by which the vulnerability or finding will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the vulnerability has been remedied or the finding addressed.

18.14 The Supplier shall promptly provide the Buyer with such technical and other information relating to the Supplier Information Management System, the IT Health Check report or the draft Remediation Action Plan as the Buyer requests.

18.15 The Buyer may:

(a) reject the draft Remediation Action Plan where it considers that the draft Remediation Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Remediation Action Plan submit a revised draft Remediation Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 18.13 to 18.15 shall apply, with appropriate modifications, to the revised draft Remediation Action Plan;

(b) accept the draft Remediation Action Plan, in which case the Supplier must immediately start work on implementing the Remediation Action Plan in accordance with Paragraph 18.16 and 18.17.

*Implementing an approved Remediation Action Plan*

18.16 In implementing the Remediation Action plan, the Supplier must conduct such further tests on the Supplier Information Management System as are required by the Remediation Action Plan to confirm that the Remediation Action Plan has fully and correctly implemented.

18.17 If any such testing identifies a new risk, new threat, vulnerability or exploitation technique with the potential to affect the security of the Supplier Information Management System, the Supplier shall within [2] Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique:

(a) provide the Buyer with a full, unedited and unredacted copy of the test report;

(b) implement interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

(c) as far as practicable, remove or disable any extraneous interfaces, services or capabilities not needed for the provision of the Services within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.



## 19 Access Control

19.1 This paragraph applies where the Buyer has assessed that this Agreement is a higherrisk agreement.

19.2 The Supplier must, and must ensure that all Sub-contractors:

(a) identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;

(b) require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.

19.3 The Supplier must ensure, and must ensure that all Sub-contractors 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 Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) in the case of a higher-risk agreement 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.

19.4 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that it logs all activity of the Privileged Users while those users access those accounts and keeps the activity logs for 20 Working Days before deletion.

19.5 The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different high-complexity passwords for their different accounts on the Supplier Information Management System.

19.6 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in paragraphs 19.2 to 19.5.

19.7 The Supplier must, and must ensure that all Sub-contractors:

(a) configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and

(b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.



## 20 Event logging and protective monitoring

*Protective Monitoring System*

20.1 The Supplier must, and must ensure that Sub-contractors, implement an effective system of monitoring and reports analysing access to and use of the Supplier Information Management System, the Development Environment, the Buyer Data and the Code to:

(a) identify and prevent potential Breaches of Security;

(b) respond effectively and in a timely manner to Breaches of Security that do occur;

(c) identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

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

20.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier Information Management 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 Buyer Data;

(c) the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques; (d) any other matters required by the Security Management Plan.

*Event logs*

20.3 The Supplier must ensure that, unless the Buyer otherwise agrees, any event logs do not log: (a) personal data, other than identifiers relating to users; or (b) sensitive data, such as credentials or security keys.

*Provision of information to Buyer*

20.4 The Supplier must provide the Buyer on request with:

(a) full details of the Protective Monitoring System it has implemented; and

(b) copies of monitoring logs and reports prepared as part of the Protective Monitoring System. *Changes to Protective Monitoring System*

20.5 The Buyer may at any time require the Supplier to update the Protective Monitoring System to: (a) respond to a specific threat identified by the Buyer;



(b) implement additional audit and monitoring requirements; and

(c) stream any specified event logs to the Buyer's security information and event management system.

## 21 Audit rights

*Right of audit*

21.1 The Buyer may undertake an audit of the Supplier or any Sub-contractor to:

(a) verify the Supplier's or Sub-contractor's (as applicable) compliance with the requirements of this Schedule [◆] (*Security Management*) and the Data Protection Laws as they apply to Buyer Data;

(b) inspect the Supplier Information Management System (or any part of it); (c) review the integrity, confidentiality and security of the Buyer Data; and/or (d) review the integrity and security of the Code.

21.2 Any audit undertaken under this Paragraph 21:

(a) may only take place during the Term and for a period of 18 months afterwards; and

(b) is in addition to any other rights of audit the Buyer has under this

Agreement.

21.3 The Buyer may not undertake more than one audit under Paragraph 21.1 in each calendar year unless the Buyer has reasonable grounds for believing:

(a) the Supplier or any Sub-contractor has not complied with its obligations under this Agreement or the Data Protection Laws as they apply to the Buyer Data; (b) there has been or is likely to be a Security Breach affecting the Buyer Data or the Code; or (c) where vulnerabilities, or potential vulnerabilities, in the Code have been identified by: (i) an IT Health Check; or

(ii) a Breach of Security.

*Conduct of audits*

21.4 The Authority must use reasonable endeavours to provide 15 Working Days' notice of an

audit. 21.5 The Authority must when conducting an audit:

(a) comply with all relevant policies and guidelines of the Supplier or Sub-contractor (as applicable) concerning access to the Suppler Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and

(b) use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

21.6 The Supplier must, and must ensure that Sub-contractors, on demand provide the Buyer with all co operation and assistance the Buyer may reasonably require, including:

(a) all information requested by the Buyer within the scope of the audit;

 (b) access

to the Supplier Information Management System; and (c)

access to the Supplier Staff.

*Response to audit findings*

21.7 Where an audit finds that:

(a) the Supplier or a Sub-contractor has not complied with this Agreement or the Data Protection Laws as they apply to the Buyer Data; or

(b) there has been or is likely to be a Security Breach affecting the Buyer Data the Buyer may require the Supplier to remedy those defaults at its own cost and expense and within the time reasonably specified by the Buyer.

21.8 The exercise by the Buyer of any rights it may have under this Paragraph 3 does not affect the exercise by it of any other or equivalent rights it may have under this Agreement in respect of the audit findings.

## 22 Breach of Security

*Reporting Breach of Security*

22.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

*Immediate steps*

22.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other steps reasonably necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of

Security; (b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause

failure; *Subsequent action*

22.3 As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security, provide to the Buyer:

(a) full details of the Breach of Security; and (b) if required by the Buyer:

(i) a root cause analysis; and

(ii) a draft plan addressing the root cause of the Breach of Security

(the "**Breach Action Plan**").

22.4 The draft Breach Action Plan must, in respect of each issue identified in the root cause

analysis: (a) how the issue will be remedied;



(b) the date by which the issue will be remedied; and

(c) the tests that the Supplier proposes to perform to confirm that the issue has been remedied or the finding addressed.

22.5 The Supplier shall promptly provide the Buyer with such technical and other information relating to the draft Breach Action Plan as the Buyer requests.

22.6 The Buyer may:

(a) reject the draft Breach Action Plan where it considers that the draft Breach Action Plan is inadequate, providing its reasons for doing so, in which case:

(i) the Supplier shall within 10 Working Days of the date on which the Buyer rejected the draft Breach Action Plan submit a revised draft Breach Action Plan that takes into account the Buyer's reasons; and

(ii) paragraph 22.5 and 22.6 shall apply to the revised draft Breach Action Plan;

(b) accept the draft Breach Action Plan, in which case the Supplier must immediately start work on implementing the Breach Action Plan.

*Assistance to Buyer*

22.7 Where the Breach of Security concerns or is connected with the Buyer Data or the Code, the Supplier must 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.

22.8 The obligation to provide assistance under Paragraph 22.7 continues notwithstanding the expiry or termination of this Contract.

*Reporting of Breach of Security to regulator*

22.9 Where the Law requires the Supplier report a Breach of Security to the appropriate regulator, the Supplier must:

(a) make that report within the time limits:

(i) specified by the relevant regulator; or

(ii) otherwise required by Law;

(b) to the extent that the relevant regulator or the Law permits, provide the Buyer with a full, unredacted and unedited copy of that report at the same time it is sent to the relevant regulator.

22.10 Where the Law requires the Buyer to report a Breach of Security to the appropriate regulator, the Supplier must:

(a) provide such information and other input as the Buyer requires within the timescales specified by the Buyer;

(b) where Paragraph 7 applies to the Breach of Security, ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.



## 23 Return and Deletion of Buyer Data

23.1 The Supplier must create and maintain a register of:

(a) all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and

(b) those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub contractor, on which the Buyer Data is stored (the "**Buyer Data Register**").

23.2 The Supplier must:

(a) review and update the Buyer Data Register:

(i) within 10 Working Days of the Supplier or any Sub-contractor changes to those parts of the Supplier Information Management System on which the Buyer Data is stored;

(ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;

(iii) at least once every 12 (twelve) months; and

(b) provide the Buyer with a copy of the Buyer Data Register: (i) whenever it updates the Buyer Data Register; and

(ii) otherwise when the Buyer requests.

23.3 The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

(a) when requested to do so by the Buyer; and

(b) using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

23.4 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code: (a) when requested to do so by the Buyer; and (b) using the method specified by the Buyer.

# 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:<br>a) Government Department;<br>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; |
| **"Buyer"** | means the person identified in the letterhead of the Order Form; |
| **"Date of Delivery"** | means that date by which the Deliverables must be delivered to 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"** | (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy; |
| **"Data Protection Impact Assessment"** | an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data; |
| **"Data Protection Officer"** | has the meaning given to it in the GDPR; |
| **"Data Subject"** | has the meaning given to it in the GDPR; |
| **"Data Loss Event"** | any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach; |
| **"Data Subject Access Request"** | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |

| | |
|---|---|
| **"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"** | any event, occurrence, circumstance, matter or cause affecting the performance by either Party of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control which prevent or materially delay it from performing its obligations under the Contract but excluding: i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds; |
| **"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: 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; |
| **"Personal Data Breach"** | has the meaning given to it in the GDPR; |
| **"Processor"** | has the meaning given to it in the GDPR; |
| **"Purchase Order Number"** | means the Buyer's unique number relating to the order for 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 2004 as relevant (where the meaning set out for the term "request" shall apply); |
| **"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 or, where applicable, the Buyer's procedures for the vetting of personnel as provided to the Supplier from time to time;

**"Subprocessor"** any third Party appointed to process Personal Data on behalf of the Supplier related to the Contract;

**"Supplier Staff"** all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;

**"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 [subsuppliers].

**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 cooperation 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 reprocurement;
(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 cooperation 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.