## 

## Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

### Order Form

Call-Off Reference: CCIT23A12

Call-Off Title: Provision of GGMF Find a Grant Development

Call-Off Contract Description: To establish a single Supplier Contract for the purchase of services for Find a Grant Development.

The Buyer: Cabinet Office

Buyer Address: **Redacted under FOIA section 40, Personal Information**

The Supplier: ANDigital Ltd

Supplier Address: **Redacted under FOIA section 40, Personal Information**

Registration Number: **Redacted under FOIA section 40, Personal Information**

DUNS Number: **Redacted under FOIA section 40, Personal Information**

SID4GOV ID: N/A

#### Applicable Framework Contract

This Order Form is for the provision of the Call-Off Deliverables and dated at 24 April 2023 Contract Award.

It’s issued under the Framework Contract with the reference number RM1043.8 for the provision of Digital Outcomes Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement of Work which shall be executed at the same time that the Call-Off Contract is executed, oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier’s Call-Off Contract.

#### Call-Off Lot

Lot 1 – Digital Outcomes

#### Call-Off Incorporated Terms

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions) RM1043.8
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

* Joint Schedules for RM1043.8
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 5 (Corporate Social Responsibility)
  + Joint Schedule 6 (Key Subcontractors)
  + Joint Schedule 7 (Financial Difficulties)
  + Joint Schedule 8 (Guarantee)
  + Joint Schedule 10 (Rectification Plan)
  + Joint Schedule 11 (Processing Data) RM1043.8
  + Joint Schedule 12 (Supply Chain Visibility)
* Call-Off Schedules for RM1043.8
  + Call-Off Schedule 1 (Transparency Reports)
  + Call-Off Schedule 2 (Staff Transfer)
  + Call-Off Schedule 3 (Continuous Improvement)
  + Call-Off Schedule 5 (Pricing Details and Expenses Policy)
  + Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)
  + Call-Off Schedule 7 (Key Supplier Staff)
  + Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  + Call-Off Schedule 9 (Security)
  + Call-Off Schedule 10 (Exit Management)
  + Call-Off Schedule 12 (Clustering)
  + Call-Off Schedule 13 (Implementation Plan and Testing)
  + Call-Off Schedule 14 (Service Levels and Balanced Scorecard)
  + Call-Off Schedule 15 (Call-Off Contract Management)
  + Call-Off Schedule 16 (Benchmarking)
  + Call-Off Schedule 17 (MOD Terms)
  + Call-Off Schedule 18 (Background Checks)
  + Call-Off Schedule 19 (Scottish Law)
  + Call-Off Schedule 20 (Call-Off Specification)
  + Call-Off Schedule 21 (Northern Ireland Law)
  + Call-Off Schedule 23 (HMRC Terms)
  + Call-Off Schedule 25 (Ethical Walls Agreement)
  + Call-Off Schedule 26 (Cyber Essentials Scheme)

1. CCS Core Terms (version 3.0.11)
2. Joint Schedule 5 (Corporate Social Responsibility) RM1043.8
3. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

#### Call-Off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:

None

Call-Off Start Date: 25/04/2023

Call-Off Expiry Date: 24/04/2024

Call-Off Initial Period: One (1) Year

Call-Off Optional Extension Period: Not applicable

Minimum Notice Period for Extensions: Not applicable

Call-Off Contract Value: £2,500,000.00

#### Call-Off Deliverables

See details held in Call-Off Schedule 20 (Call-Off Specification)

#### Warranty Period

The Supplier shall provide digital and Software Deliverables with a minimum warranty of at least 90 days against all obvious defects, and in relation to the warranties detailed in Paragraphs 4 (licensed Software warranty) and 9.6.2 (Specially Written Software and New IPRs) of Call-Off Schedule 6 (IPRs and Additional Terms on Digital Deliverables).

#### Buyer’s Standards

From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards referred to in Framework Schedule 1 (Specification).

#### Cyber Essentials Scheme

The Buyer requires the Supplier, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

#### Maximum Liability

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £2,500,000

#### Call-Off Charges

Capped Time and Materials (CTM)

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

All changes to the Charges must use procedures that are equivalent to those in Paragraph 4 in Framework Schedule 3 (Framework Prices).]

#### Reimbursable Expenses

Expenses may be claimed by the Supplier when the Buyer requires the Supplier’s personnel to travel outside of the programme base, which is Glasgow. Any such expenses should be approved by the Buyer in advance.

#### Payment Method

* + - 1. Invoices should be emailed to:

#### Buyer’s Invoice Address

#### Redacted under FOIA section 40, Personal Information

#### Buyer’s Environmental Policy

Redacted under FOIA section 40, Personal Information

#### Buyer’s Security Policy

Appended at Annex 2

#### Supplier’s Authorised Representative

#### Redacted under FOIA section 40, Personal Information

#### Supplier’s Contract Manager

Redacted under FOIA section 40, Personal Information G2 1QQ

#### Progress Report Frequency

On the first Working Day of each calendar month

#### Progress Meeting Frequency

Quarterly on the first Working Day of each quarter

#### Key Staff

Redacted under FOIA section 40, Personal Information

#### Key Subcontractor(s)

#### Not applicable

#### Commercially Sensitive Information

Redacted under FOIA section 43, Commercial Interests

#### Balanced Scorecard

Not applicable

#### Material KPIs

The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14 (Service Levels and Balanced Scorecard):

|  |  |  |
| --- | --- | --- |
| **Material KPIs** | **Target** | **Measured by** |
| All key technical roles are filled by suitably qualified and security-cleared personnel, with no gaps that impact delivery | Maximum 2 weeks onboarding new personnel | Resources confirmed in weekly contract meetings |
| Plans showing the roadmap towards the key deliverables are produced within one month of the contract start | End May | Plans confirmed in weekly contract meetings |
| Sprint plans are shared and agreed with the Cabinet Office in advance of each sprint | Fortnightly | Scope confirmed in weekly contract meetings |
| Deliverables are developed in compliance with the Government's Digital Service Standard<https://www.gov.uk/service-manual/service-standard> | Ongoing | Service assessments |

#### Service Credits

Not applicable

#### Additional Insurances

Not applicable

#### Guarantee

Not applicable

#### Social Value Commitment

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)

#### Statement of Works

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

**For and on behalf of the Supplier:**

Signature: Redacted under FOIA section 40, Personal Information

Name: Redacted under FOIA section 40, Personal Information

Role: Redacted under FOIA section 40, Personal Information

Date: 19th May 20233

**For and on behalf of the Buyer:**

Signature: Redacted under FOIA section 40, Personal Information

Name: Redacted under FOIA section 40, Personal Information

Role: Redacted under FOIA section 40, Personal Information

Date: Redacted under FOIA section 40, Personal Information

### Annex 1 (Template Statement of Work)

1. **Statement of Works (SOW) Details**

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.

All SOWs must fall within the Specification and provisions of the Call-Off Contact.

The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.

**Date of SOW:**

**SOW Title:**

**SOW Reference:**

**Call-Off Contract Reference:**

**Buyer:**

**Supplier:**

**SOW Start Date:**

**SOW End Date:**

**Duration of SOW:**

**Key Personnel (Buyer):**

**Key Personnel (Supplier):**

**Subcontractors:**

1. **Call-Off Contract Specification – Deliverables Context**

**SOW Deliverables Background**: [**Insert** details of which elements of the Deliverables this SOW will address]

**Delivery phase(s)**: [**Insert** item and nature of Delivery phase(s), for example, Discovery, Alpha, Beta or Live]

**Overview of Requirement**: [**Insert** details including Release Type(s), for example Ad hoc, Inception, Calibration or Delivery]

1. **Buyer Requirements – SOW Deliverables**

**Outcome Description:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Milestone Ref** | **Milestone Description** | **Acceptance Criteria** | **Due Date** |
| MS01 |  |  |  |
| MS02 |  |  |  |

**Delivery Plan:**

**Dependencies:**

**Supplier Resource Plan:**

**Security Applicable to SOW:**

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security).

[If different security requirements than those set out in Call-Off Schedule 9 (Security) apply under this SOW, these shall be detailed below and apply only to this SOW:

[**Insert if necessary]**

**Cyber Essentials Scheme:**

The Buyer requires the Supplier to have and maintain a **Cyber Essentials Certificate** for the work undertaken under this SOW, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme).

**SOW Standards:**

[**Insert** any specific Standards applicable to this SOW]

**Performance Management:**

[**Insert** details of Material KPIs that have a material impact on Contract performance]

|  |  |  |
| --- | --- | --- |
| **Material KPIs** | **Target** | **Measured by** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

[**Insert** Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)]

**Additional Requirements:**

**Annex** **1** – Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex 1 attached to this Statement of Work.

**Key Supplier Staff:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Role** | **Key Staff** | **Contract Details** | **Worker Engagement Route (incl. inside/outside IR35)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[**Indicate**: whether there is any requirement to issue a Status Determination Statement]

**SOW Reporting Requirements:**

Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref.** | **Type of Information** | **Which Services does this requirement apply to?** | **Required regularity of Submission** |
| 1. | [**insert**] | | |
| 1.1 | [insert] | [insert] | [insert] |

1. **Charges**

**Call Off Contract Charges:**

The applicable charging method(s) for this SOW is:

* Capped Time and Materials

**Rate Cards Applicable:**

[**Insert** SOW applicable Supplier and Subcontractor rate cards from Call-Off Schedule 5 (Pricing Details and Expenses Policy), including details of any discounts that will be applied to the work undertaken under this SOW.]

**Reimbursable Expenses:**

None

1. **Signatures and Approvals**

**Agreement of this SOW**

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:

**For and on behalf of the Supplier**

Name:

Title:

Date:

Signature:

**For and on behalf of the Buyer**

Name:

Title:

Date:

Signature:

### Annex 1

### Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 do not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

Template Annex 1 of Joint Schedule 11 (Processing Data) Below

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:   * [**Insert** the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority]   **The Supplier is Controller and the Relevant Authority is Processor**  The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:   * [**Insert** the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier]   **The Parties are Joint Controllers**  The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:   * [**Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]   **The Parties are Independent Controllers of Personal Data**  The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:   * Business contact details of Supplier Personnel for which the Supplier is the Controller, * Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority’s duties under the Contract) for which the Relevant Authority is the Controller, * [**Insert** the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority]   [**Guidance** where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified] |
| Duration of the Processing | [Clearly set out the duration of the Processing including dates] |
| Nature and purposes of the Processing | [Be as specific as possible, but make sure that you cover all intended purposes.  The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.  The purpose might include: employment processing, statutory obligation, recruitment assessment etc.] |
| Type of Personal Data | [Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.] |
| Categories of Data Subject | [Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.] |
| Plan for return and destruction of the data once the Processing is complete  UNLESS requirement under Union or Member State law to preserve that type of data | [Describe how long the data will be retained for, how it be returned or destroyed] |

# Annex 2 Schedule: Security Management:

|  |  |
| --- | --- |
| “Anti-virus Software” | means software that:  (a) protects the Supplier Information Management System from the possible introduction of Malicious Software;  (b) scans for and identifies possible Malicious Software in the Supplier Information Management System;  (c) if Malicious Software is detected in the Supplier Information Management System, so far as possible:  (i) prevents the harmful effects of the Malicious Software; and  (ii) removes the Malicious Software from the Supplier Information Management System; |
| “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;  (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or  (c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; |
| “Buyer Data” | means (d) 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; or  (e) Personal Data for which the Buyer is a, or the, Data Controller,  that is:  (a) supplied to the Supplier by or on behalf of the Buyer; or  (b) that the Supplier generates, processes, stores or transmits under this Agreement. |
| “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 86; |
| “Certification Rectification Plan” | means the plan referred to in Paragraph 92; |
| “Certification Requirements” | means the information security requirements set out in paragraph 75. |
| “CHECK Service Provider” | means a company certified by the NCSC to conduct authorised penetration tests of public sector and CNI systems and networks. |
| “Code” | means, in respect of the Developed System:  (a) the source code;  (b) the object code;  (c) third-party components, including third-party coding frameworks and libraries; and  all supporting documentation. |
| “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;  (d) deployment; and  (e) maintenance. |
| “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. |
| “End-user Device” | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services. |
| “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; |
| “Malicious Software” | means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations; |
| ‘NCSC Cloud Security Principles” | means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles. |
| “NCSC Device Guidance” | means the National Cyber Security Centre’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 Secure Design Principles” | means the National Cyber Security Centre’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/cyber-security-design-principles; |
| “NCSC Secure Development Guidance” | means the National Cyber Security Centre’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; |
| “Privileged User” | means a user with system administration access to the Supplier Information Management System or the Developed 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 1.6 of Annex 1. |
| “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:  (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);  (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:  (i) full legal name;  (ii) trading name (if any)  (iii) country of registration;  (iv) registration number (if applicable); and  registered address. |
| “Relevant Activities” | means those activities specified in Annex 1. |
| “Relevant Certifications” | means those certifications specified in Paragraph 76; |
| “Relevant Convictions” | means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), [driving offences, offences against property, drugs, alcohol, public order offences] or any other offences relevant to Services as the Buyer may specify; |
| “Security Management Plan” | means the document prepared in accordance with the requirements of Paragraph 100 |
| “Sites” | means any premises:  (a) from or at which:  (i) the Services are (or are to be) provided; or  (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or  (b) where:  (i) any part of the Supplier Information Management System is situated; or  (ii) any physical interface with the Buyer System takes place; |
| “Standard Contractual Clauses” | means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area; |
| “Supplier Information Management System” | means:  (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; and  (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); |
| “Sub-contractor Personnel” | means:  (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and  (b) engaged in or likely to be engaged in:  (i) the performance or management of the Services;  (ii) or the provision of facilities or services that are necessary for the provision of the Services. |
| “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; |
| “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; |

# 46. Introduction

## 47. This Schedule, Security Management sets out:

### 48. 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 the Buyer Data, the Services, the Developed System and the Supplier Information Management System;

### 49. the assessment of this Agreement as

#### 50. Higher-risk consultancy agreement,

#### 50.1.1.1 in Paragraph 4;

### 51. the Buyer’s access to the Supplier Personnel and Supplier Information Management System, in Paragraph 5;

### 52. the Certification Requirements, in Paragraph 6;

### 53. the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in Paragraph 100;

### 54. the security requirements with which the Supplier must comply in Annex 1;

# 55. Principles of Security

## 56. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:

### 57. the Sites;

### 58. the Services;

### 59. the Supplier’s Information Management System; and

### 60. The Developed System.

## 61. Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System and the Developed System, the Supplier remains responsible for:

### 62. 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; and

### 63. the security of the Supplier Information Management System and the Developed System.

## 64. The Supplier shall:

### 65. comply with the security requirements in Annex 1; and

## 66. 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.

# 67. Buyer Risk Assessment

## 68. The Buyer has assessed this Agreement as

### 68.1.1 x□ A higher risk consultancy agreement;

# 69. Access to Supplier Personnel and Supplier Information Management System

## 70. The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

### 71. access to the Supplier Personnel;

### 72. access to the Information Management System to audit the Supplier and its Sub-contractors’ compliance with this Agreement; and

### 73. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

## 73.1 to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data, the Developed System and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

## 74. The Supplier must provide the access required by the Buyer in accordance with Paragraph 5.1 within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 of receipt of such request.

# 75. Certification Requirements

## 76. The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

### 77. In the case of a standard consultancy agreement:

## 77.1 [Buyer to check as appropriate]

### 77.1.1 □ Cyber Essentials Plus;

### 77.1.2 □ Cyber Essentials; or

### 78. In the case of a higher-risk consultancy agreement:

#### 79. 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 when this becomes fully available; It is acknowledged by the buyer that the supplier is not fully certified in relation to ISO27001 however the supplier has confirmed that this is actively being progressed.

#### 80. Cyber Essentials Plus (the “Relevant Certifications”).

## 81. Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

## 82. The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

### 83. Currently in effect;

### 84. Relate to the full scope of the Supplier Information System; and

### 85. Are not subject to any condition that may impact the provision of the Services.

## 86. The Supplier must notify the Buyer promptly, any in any event within three (3) Working Days of becoming aware that:

### 87. A Relevant Certification has been revoked or cancelled by the body that awarded it;

### 88. A Relevant Certification expired and has not been renewed by the Supplier;

### 89. A Relevant Certification no longer applies to the full scope of the Supplier Information Management System or

### 90. 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”)

## 91. Where the Supplier has notified the Buyer of a Certification Default under Paragraph 86:

### 92. the Supplier must, within 10 working Days of the date in which the Supplier provided notice under Paragraph 86 (or such other period as the Parties may agree) provide a draft plan (a “Certification Rectification Plan”) to the Supplier setting out:

#### 93. full details of the Certification Default, including a root cause analysis;

#### 94. the actual and anticipated effects of the Certification Default;

#### 95. the steps the Supplier will take to remedy the Certification Default;

### 96. the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

### 97. If the Buyer rejects the Certification Rectification Plan, the Buyer must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph 96 will apply to the re-submitted plan;

### 98. The rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

### 99. If the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

# 100. Security Management Plan

## *100.1* *Preparation of Security Management Plan*

## 101. This Paragraph 100 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

## 102. 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 [x] (Security Management) and the Agreement in order to ensure the security of the Buyer Data, the Developed System and the Supplier Information Management System.

## 103. The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

### 104. an assessment of the Supplier Information Management System against the requirements of this Schedule, Security Management, including the Annexes;

### 105. 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 Buyer Data, the Buyer, the Services and/or users of the Services; and

### 106. the following information in respect of each Sub-contractor:

#### 107. the Sub-contractor’s:

##### 108. Legal name;

##### 109. Trading name (if any);

##### 110. Registration details (where the Sub-contractor is not an individual);

#### 111. the Sites used by the Sub-contractor;

#### 112. the Buyer Data Processed by the Sub-contractor;

#### 113. the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

#### 114. the measures the Sub-contractor has in place to comply with the requirements of this Schedule, Security Management.

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

### 116. an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or

### 117. a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

## 118. 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.

## *118.1* *Updating Security Management Plan*

## 119. 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.

## *119.1* *Monitoring*

## 120. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

### 121. a significant change to the components or architecture of the Supplier Information Management System;

### 122. a new risk to the components or architecture of the Supplier Information Management System;

### 123. a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

### 124. a change in the threat profile;

### 125. a significant change to any risk component;

### 126. a significant change in the quantity of Personal Data held within the Service;

### 127. a proposal to change any of the Sites from which any part of the Services are provided; and/or

### 128. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

## 129. 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.