RM6102 CONTRACT ORDER FORM

This Contract Order Form is issued in accordance with the provisions of the Apprenticeship Training Provider Dynamic Marketplace (DMP) Agreement for the provision of Apprenticeship Training and related Services. Dated 30 January 2024
.

The Supplier agrees to supply the Goods and/or Services specified below on and subject to the terms of this Contract.

For the avoidance of doubt this Contract consists of the terms set out in this Contract Order Form and the Contract Terms.

Order Number	CCDE23A14 - Lot 2 Level 4 DevOps Engineer – ST0825
From	The Cabinet Office 70 Whitehall London SW1A 2AS ("Customer")
To	Makers Academy Zetland House 5-25 Scrutton Street London EC2A 4HJ ("Supplier")

1. **CONTRACT PERIOD**

1.1	Commencement Date	16 February 2024
1.2	Expiry Date	Initial Term 3 years; Expiry date: 15 February 2027 Option to extend by two periods of one year

2. **SERVICES REQUIRED**

2.1	**Services Required:** Apprenticeship training provider services / end point Assessor Services / Both. **Location:** Apprenticeship type and specific applicable institute for apprenticeships standard	Apprenticeship training provider services and end point Assessor Services See Annex 1 in Contract Schedule 2 The Services for full services required. UK Wide Level 4 DevOps Engineer – ST0825

	Number of students Class based Additional services	To be confirmed Various delivery options – see Annex 1 in Contract Schedule 2 The Services. See Appendix A Special Terms

3. **CONTRACT PERFORMANCE**

3.1	Required Apprenticeship Standard	Continued adherence to the relevant Institute for Apprenticeships industry standard. (www.instituteforapprenticeships.org/) Maintained ESFA registration and accreditation. General industry good practice

3.1	Quality Standards	The Suppliers shall be registered on the Education and Skills Funding Agency (ESFA) Register of Apprenticeship Training Providers (RoATP) via the main application route and shall deliver the services in accordance with Apprenticeship funding and performance-management rules for Training Providers. Further information can be found at: https://www.gov.uk/guidance/apprenticeship-funding-rules The Suppliers shall have in place a financial strategy that is simple, clear and in line with Department for Education (formerly BIS/ESFA) funding rules. The full DfE rules can be found at: apprenticeship-funding-from-may-2017. The Suppliers shall select the End Point Assessment (EPA), from the Register of Apprentice Assessment Organisations (RoAAO). The list can be found at: https://www.gov.uk/guidance/register-of-end-point-assessment-organisations

4. **PAYMENT**

4.1	Contract Charges	See Annex 1 Contract Charges of Contract Schedule 3. The total Contract value shall not exceed £8,075,000 (excluding VAT and any extension options)

4.2	Payment terms/Profile	Payment to be made in accordance with the current in force ESFA funding rules. Further additional terms in Annex 2 of Contract Schedule 3.
4.3	Customer billing address	To be confirmed by the Contracting Authority

5. **LIABILITY AND INSURANCE**

5.1	Suppliers' limitation of Liability	In Clause 25 of the Contract Terms
5.2	Insurance	Professional Indemnity Insurance cover of £1,000,000.00 for any one claim. Public Liability Insurance cover of £1,000,000.00 for any one claim. Employers Liability insurance cover of £5,000,000.00 for any one claim.

FORMATION OF CONTRACT

By signing and completing this Contract Order Form the Supplier and the Customer agree to enter into a binding contract governed by the terms of this Contract Order Form and the attached terms and conditions which includes Appendix 1 to the Order Form (Special Terms Schedule).

Order Number	**CCDE23A14**
Signed - via Docusign	
Supplier: <Supplier Sign & Date below (name & job title)> **REDACTED TEXT under FOIA Section 40, Personal Information**.	
Buyer: <Commercial Sign & Date below (name & job title)> **REDACTED TEXT under FOIA Section 40, Personal Information**.	

Order Number	CCDE23A14
Signed - via Docusign	

Appendix 1 – Special Terms Schedule

FOR

Dynamic Marketplace RM6102 - For the Provision of Apprenticeship Training and Related Services

CONTRACT REFERENCE NUMBER: CCDE23A14 Tech Track Apprenticeship Training and Related Services

Cabinet Office

CONTENTS:

Part A	3
DEFINITIONS	3
Part B – Security and Assurance Requirements	7
1. ASSURANCE REQUIREMENTS	7
2. SUPPLIER OBLIGATIONS	7
3. CERTIFICATION REQUIREMENTS	9
Annex 1: Security Management Plan Template	19
Part C – Data Processing	20
Part D – Contract Schedule 7: Processing Person Data and Data Subjects	22
1. Processing Data	22
2. Independent Controllers of Personal Data	24
3. Joint Controllers	26
Part E – Joint Controller Agreement	

Part A - Definitions

"Anti-virus Software"	means software that: (a) protects the Supplier System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier System; (c) if Malicious Software is detected in the Supplier System, so far as possible:

	(i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier System;
"Contract Year"	means: (a) a period of 12 months commencing on the Effective Date; (b) thereafter a period of 12 months commencing on each anniversary of the Effective Date; (c) with the final Contract Year ending on the expiry or termination of the Term;
"CREST Service Provider"	means a company with an information security accreditation of a security operations centre qualification from CREST International;
"Government Data"	means any: (a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; (b) Personal Data for which the Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in paragraphs (a) or (b); that is: (d) supplied to the Supplier by or on behalf of the Buyer; or (e) that the Supplier generates, processes, stores or transmits under this Agreement; and for the avoidance of doubt includes the Code and any meta-data relating to the Code.
"Certifications"	means one or more of the following certifications: (b) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and (c) Cyber Essentials Plus; and/or (d) Cyber Essentials;
"Breach of Security"	means the occurrence of: (a) any unauthorised access to or use of the

	Services, the Sites, the Supplier System and/or the Government Data; (b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or (c) any part of the Supplier System ceasing to be compliant with the required Certifications; (d) the installation of Malicious Software in the Supplier System: (e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and (f) includes any attempt to undertake the activities listed in sub-paragraph (a) where the Supplier has reasonable grounds to suspect that attempt: (i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or (ii) was undertaken, or directed by, a state other than the United Kingdom;
"CHECK Scheme"	means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
"CHECK Service Provider"	means a company which, under the CHECK Scheme: (a) has been certified by the NCSC; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by Paragraph 5.2 (*Security Testing*);
"Cloud Security Principles"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;

“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the NCSC;
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
“IT Health Check”	means testing of the Supplier Information Management System by a CHECK Service Provider;
“Malicious Software”	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
“NCSC”	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
“NCSC Device Guidance”	means the NCSC’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
“Privileged User”	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
“Process”	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
“Prohibition Notice”	means the meaning given to that term by Paragraph 4.4.
“Protective Monitoring System”	has the meaning given to that term by Paragraph 13.1;
“Relevant Conviction”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
“Sites”	means any premises (including the Buyer’s Premises, the Supplier’s premises or third-party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or

	(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated; or (ii) any physical interface with the Authority System takes place;
"Standard Contractual Clauses"	means, for the purposes of this Schedule 4, Annex 1 (*Security Management*): (a) the standard data protection paragraphs specified in Article 46 of the UK GDPR setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area; (b) as modified to apply equally to the Government Data as if the Government Data were Personal Data;
"Subcontractor Personnel"	means: (a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and (b) engaged in or likely to be engaged in: (i) the performance or management of the Services; or (ii) the provision of facilities or services that are necessary for the provision of the Services;
"Supplier System"	means (a) any: (i) information assets, (ii) IT systems, (iii) IT services; or (iv) Sites, that the Supplier or any Subcontractor will use to Process, or support the Processing of, Government Data and provide, or support the provision of, the Services; and (b) the associated information management system, including all relevant: (i) organisational structure diagrams; (ii) controls;

	(iii) policies; (iv) practices; (v) procedures; (vi) processes; and (vii) resources;
"Third-party Tool"	means any activity conducted other than by the Supplier during which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;

Part B – Security and Assurance Requirements

1. ASSURANCE REQUIREMENTS

Introduction

1.1 The reference to 'Attachment 6 of this Contract' in paragraph 16.1 of Contract Schedule 2: Goods and/or Services, shall be read as a reference to this Part B of Appendix 1.

a) 2. Supplier obligations

Core requirements

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

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

Certifications (see Paragraph 3)		
The Supplier must have the following Certifications:	ISO/IEC 27001:2013 by a UKAS-approved certification body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☒
Subcontractors that Process Government Data must have the following Certifications:	ISO/IEC 27001:2013 by a UKAS-approved certification body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☒
Locations (see Paragraph 4)		

The Supplier and Subcontractors may store, access or Process Government Data in:	the United Kingdom only	☐
	the United Kingdom and European Economic Area only	☒
	anywhere in the world not prohibited by the Buyer	☐

Optional requirements

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

Security testing (see Paragraph 9)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☒
Cloud Security Principles (see Paragraph 10)	
The Supplier must assess the Supplier System against the Cloud Security Principles	☒
Record keeping (see paragraph 11)	
The Supplier must keep records relating to Subcontractors, Sites, Third Party Tools and third parties	☒
Encryption (see Paragraph 12)	
The Supplier must encrypt Government Data while at rest or in transit	☒
Protecting Monitoring System (see Paragraph 13)	
The Supplier must implement an effective Protective Monitoring System	☒
Patching (see Paragraph 14)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☒
Malware protection (see Paragraph 15)	
The Supplier must use appropriate Anti-virus Software	☒
End-user Devices (see Paragraph 16)	
The Supplier must manage End-user Devices appropriately	☒
Vulnerability scanning (see Paragraph 17)	

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

Part One: Core Requirements

Certification Requirements

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

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

(a) it; and

(b) any Subcontractor that Processes Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1:

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

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

(b) throughout the Term.

2 Location

2.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Process Government Data outside the United Kingdom.

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

2.3 Where the Buyer has permitted the Supplier and its Subcontractors to store, access or process Government Data outside the United Kingdom or European Economic Area, the Supplier must, and must ensure that its Subcontractors store, access or process Government Data in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);

(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);

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

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

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule 4, Annex 1 (*Security Management*);

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

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

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

3 Staff vetting

3.1 **The Supplier must not allow Supplier Personnel, and must ensure that Subcontractors do not allow Subcontractor Personnel, to access or Process Government Data, if that person:**

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

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

(i) **has not undergone the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:**

(A) **the individual's identity;**

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

(C) **the individual's previous employment history; and**

(D) **that the individual has no Relevant Convictions; and**

(ii) **has not undergone national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify**

4 Supplier assurance letter

4.1 **The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its Chief Technology Officer (or equivalent officer) confirming that, having made due and careful enquiry:**

(a) **the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Agreement;**

(b) **it has fully complied with all requirements of this Schedule 4, Annex 1 (Security Management); and**

(c) **all Subcontractors have complied with the requirements of this Schedule 4, Annex 1 (Security Management) with which the Supplier is required to ensure they comply;**

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

5 Assurance

5.1 **The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Schedule 4, Annex 1 (*Security Management*).**

5.2 The Supplier must provide that information and those documents:

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

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

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

6 Use of Subcontractors and third parties

6.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Process Government Data comply with the requirements of this Schedule 4, Annex 1 (Security Management).

Part Two: Additional Requirements

7 Security testing

7.1 The Supplier must:

(a) before Processing Government Data;

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

undertake the following activities:

(c) conduct security testing of the Supplier System (an "IT Health Check") in accordance with Paragraph 9.2; and

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

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

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

(b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

(c) ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Process or manage Government Data; and

(d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

7.3 The Supplier treat any vulnerabilities as follows:

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

(i) if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(a)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

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

(i) if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

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

(i) if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 9.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

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

8 Cloud Security Principles

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

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

(a) before Processing Government Data;

(b) at least once each Contract Year; and

(c) when required by the Buyer.

8.3 The Supplier must:

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

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

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

9.1 The Supplier must keep the following records:

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

(i) the Subcontractor or third party's name:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual), including:

(1) country of registration;

(2) registration number (if applicable); and

(3) registered address;

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

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

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

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

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

(vii) the measures the Subcontractor or third party has in place to comply with the requirements of this Schedule 4, Annex 1 (*Security Management*);

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

(i) the location of the Site;

(ii) the operator of the Site, including the operator's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual);

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

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

(c) for Third Party Tools:

(i) the name of the Third-Party Tool;

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

(iii) in respect of the entity providing the Third-Party Tool, its:

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

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

(a) at least four times each Contract Year;

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

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

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

10 Encryption

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

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

(b) when transmitted.

11 Protective monitoring system

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

(a) identify and prevent any potential Breach of Security;

(b) respond effectively and in a timely manner to any Breach of Security that does;

(c) identify and implement changes to the Supplier System to prevent future any Breach of Security; and

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

(the "Protective Monitoring System").

11.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier System; and

(b) regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

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

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

12 Patching

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

(a) the Supplier must patch any vulnerabilities classified as "critical":

(i) if it is technically feasible to do so, within 5 Working Days of the public release; or

(ii) if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as "important":

(i) if it is technically feasible to do so, within 1 month of the public release; or

(ii) if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 14.1(b)(i), then as soon as reasonably practicable after the public release;

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

(i) if it is technically feasible to do so, within 2 months of the public release; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 14.1(c)(i), then as soon as reasonably practicable after the public release;

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

13 Malware protection

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

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

(a) prevents the installation of the most common forms of Malicious Software in the Supplier System;

(b) performs regular scans of the Supplier System to check for Malicious Software; and

(c) where Malicious Software has been introduced into the Supplier System, so far as practicable

(i) prevents the harmful effects from the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System.

14 End-user Devices

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

(a) the operating system and any applications that store, process or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Government Data must be encrypted using a suitable encryption tool;

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

(e) **the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;**

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

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

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

15 Vulnerability scanning

15.1 **The Supplier must:**

(a) **scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and**

(b) **if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 14.**

16 Access control

16.1 **The Supplier must, and must ensure that all Subcontractors:**

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

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

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

(d) **maintain records detailing each person's access to the Supplier System.**

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

(a) **are allocated to a single, individual user;**

(b) **are accessible only from dedicated End-user Devices;**

(c) **are configured so that those accounts can only be used for system administration tasks;**

(d) **require passwords with high complexity that are changed regularly;**

(e) **automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and**

(f) **are:**

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

(ii) time limited; and

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

17 Return and deletion of Government Data

17.1 When requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

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

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

18 Physical security

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

19 Breach of security

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

(a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours.

(b) provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction.

(c) where the Law requires the Buyer to report a Breach of Security to the appropriate regulator and provide such information and other input as the Buyer requires within the timescales specified by the Buyer.

20 Security Management Plan

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

Preparation of Security Management Plan

20.2 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule 4, Annex 1 (*Security Management*) and the Agreement in order to ensure the security of the Supplier solution and the Buyer data.

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

Approval of Security Management Plan

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

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

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

20.5 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.

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

Updating Security Management Plan

20.7 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

20.8 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.

20.9 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 Management Plan Template

https://docs.google.com/document/d/1LNLrrxQsQsRkkiHXaamPDtFPc4HsAWQp/edit?usp=drive_web&ouid=113392167540958834148&rtpof=true

Part C – Data Processing

1. General Provisions

1.1 **The provisions in Part D of this Schedule shall constitute Contract Schedule 7 of the Call-off Terms.**

1.2 **Where the table in Part D of this Schedule specifies that the Parties are Joint Controllers of Personal Data, the Parties shall use the Joint Controller Agreement in Part E of this Schedule at Schedule 8 to the Contract.**

1.3 **The definition of "GDPR" used in the Contract shall be read as a reference to "UK GDPR" which means: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019."**

1.4 **The defined term "Protected Measures" in Contract Schedule 1 (Definitions) shall be read as the defined term being "Protective Measures."**

1.5 **Clause 23.28(d) is deleted and replaced with the following:**

d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the UK GDPR (or section 73 of DPA 2018); or

b) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (**the "Addendum"),** as published by the Information Commissioner's Office from time to time, as well as any additional measures determined by the Controller;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

1.6 **New clause 23.28(f) is added as follows:**

f) where the Personal Data is subject to EU GDPR, not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the EU GDPR; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the non-transferring Party;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

Part D – Contract Schedule 7: Processing Person Data and Data Subjects

1. **Processing Data**

1.1 **This Schedule shall be completed by the Controllers.**

1.2 **The contact details of the Customer's Data Protection Officer are: REDACTED**

1.3 **The contact details of the Supplier's Data Protection Officer are: REDACTED**

Description	Details
Identity of the Controllers for each category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor for all data processed to provide the Services.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to Apprentices working for the Civil Service
Duration of the processing	Duration of the contract
Nature and purposes of the processing	The nature of the processing includes the 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). The purpose of the processing is to support the delivery and completion of an Apprenticeship standard.
Type of Personal Data being Processed	Name, email Address, Telephone Number, Job Title, Employer, Staff Number, Reasonable Adjustments / Disabilities, Opinions, Progression On Programme, Exam Results
Categories of Data Subject	Civil Servants

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	All data to be returned or deleted before the termination or expiry of the contract
Locations at which the Supplier and/or its Subcontractors process Personal Data under this Contract	Suppliers & Buyer's premises.
Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach	TBC by Supplier

2. **Independent Controllers of Personal Data**

2.1 **With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller and with the following clauses of Paragraph 2 of this Part D of Appendix 1.**

2.2 **Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.**

2.3 **Where a Party has provided Personal Data to the other Party in accordance with Paragraph 2.2 of this Part D of Appendix 1 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.**

2.4 **The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.**

2.5 **The Parties shall only provide Personal Data to each other:**

to the extent necessary to perform their respective obligations under the Contract;

in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

where it has recorded it in the table in Paragraph 1 of this Part D of Appendix 1.

2.6 **Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.**

2.7 **A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.**

2.8 **Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract ("Request Recipient"):**

a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) **promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and**

(ii) **provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.**

2.9 **Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:**

a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

b) implement any measures necessary to restore the security of any compromised Personal Data;

c) work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

2.10 **Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in this Part D of Appendix 1.**

2.11 **Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in this Part D of Appendix 1.**

2.12 **Notwithstanding the general application of Clauses 23.25 to 23.39 of this Contract to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 2.1 to 2.12 of this Part D of Appendix 1.**

3. **Joint Controllers**

3.1 **In respect of the Personal Data for which the Parties are Joint Controllers under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Schedule 8 (Joint Controller Agreement).**

Part E – Joint Controller Agreement

SCHEDULE 8

JOINT CONTROLLER AGREEMENT

DO NOT USE

1. **Joint Controller Status and Allocation of Responsibilities**

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Schedule 8 (Joint Controller Agreement) in replacement of Clauses 23.25 to 23.39 of the Contract and Part 2 of Contract Schedule 7 (Independent Controllers of Personal Data) as set out in Part 2 of Appendix 1 to the Contract Order Form. Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Customer:

1.2.1 is the exclusive point of contact for Data Subjects and is responsible for using all reasonable endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

1.2.2 shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

1.2.3 is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

1.2.5 shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the Customer's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of Paragraph 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. **Undertakings of both Parties**

2.1 The Supplier and the Customer each undertake that they shall:

~~2.1.1~~ report to the other Party every 3 months on:

a) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

b) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

c) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

d) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

e) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

2.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1.1(a) to (e);

2.1.3 provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 2.1.1(c) to (e) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

2.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

2.1.5 request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

2.1.6 ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

2.1.7 use all reasonable endeavours to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

a) are aware of and comply with their duties under this Schedule 8 (Joint Controller Agreement) and those in respect of Confidential Information;

b) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

c) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

2.1.8 ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

a) nature of the data to be protected;

b) harm that might result from a Personal Data Breach;

c) state of technological development; and

d) cost of implementing any measures;

2.1.9 ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

2.1.10 ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach;

2.1.11 where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the UK GDPR or DPA 2018 Section 73; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

2.1.12 where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of non-transferring Party has been obtained and the following conditions are fulfilled:

a) the transfer is in accordance with Article 45 of the EU GDPR; or

b) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU as well as any additional measures;

c) the Data Subject has enforceable rights and effective legal remedies;

d) the transferring Party complies with its obligations under the EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. **Data Protection Breach**

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Buyer and its advisors with:

3.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

3.1.2 all reasonable assistance, including:

a) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

b) co-operation with the other Party including using such reasonable endeavours as are directed by the Buyer to assist in the investigation, mitigation and remediation of a Personal Data Breach;

c) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

d) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Paragraph 3.2.

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

3.2.1 the nature of the Personal Data Breach;

3.2.2 the nature of Personal Data affected;

3.2.3 the categories and number of Data Subjects concerned;

3.2.4 the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

3.2.5 measures taken or proposed to be taken to address the Personal Data Breach; and

3.2.6 describe the likely consequences of the Personal Data Breach.

4. **Audit**

4.1 The Supplier shall permit:

4.1.1 the Customer, or a third-party auditor acting under the Customer's direction, to conduct, at the Customer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Schedule 8 and the Data Protection Legislation; and/or

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

4.2 The Customer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

The Parties shall:

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

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

6. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Customer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. **Liabilities for Data Protection Breach**

7.1 If financial penalties are imposed by the Information Commissioner on either the Customer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

7.1.1 if in the view of the Information Commissioner, the Customer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Customer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Customer, then the Customer shall be responsible for the payment of such Financial Penalties. In this case, the Customer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Customer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

7.1.2 if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Customer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Customer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

7.1.3 if no view as to responsibility is expressed by the Information Commissioner, then the Customer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Contract Schedule 6 (Dispute Resolution Procedure).

7.2 If either the Customer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "**Claim Losses**"):

7.3.1 if the Customer is responsible for the relevant Personal Data Breach, then the Customer shall be responsible for the Claim Losses;

7.3.2 if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

7.3.3 if responsibility for the relevant Personal Data Breach is unclear, then the Customer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either Paragraph 7.2 or Paragraph 7.3 shall preclude the Customer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or

claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Customer.

8. **Termination**

8.1 If the Supplier is in material Default under any of its obligations under this Schedule 8 (Joint Controller Agreement), the Customer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 30 of the Contract (Customer Termination Rights).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

9.1.1 **carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and**

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

10. Data Retention

10.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.