SCHEDULE 1

Data Processor Agreement ("the Agreement")

AGREEMENT

between

(1) AUDIT SCOTLAND, established by the Public Finance and Accountability (Scotland) Act 2000 and having its head office at 102 West Port, Edinburgh EH3 9DN (the "**Controller**"); and

(2) [ ] (the "**Processor**").

WHEREAS the Controller processes Personal Data in connection with its business activities; and whereas the Controller has engaged the services of the Processor to process Personal Data on its behalf in relation to the Contract, the parties do hereby agree as follows:-

1. DEFINITIONS AND INTERPRETATIONS

1.1 In this Agreement all words and phrases shall have the meanings provided in the Audit Scotland Terms and Conditions for the Purchase of Goods and Services and as follows:-

"National Law" shall mean the law of the Member State in which the Processor is established;

"Personal Data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to a name, an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"Processing" shall mean any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"Sub-contract" and "Sub-contracting" shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted; and

"Technical and Organisational Security Measures" shall mean all reasonable measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored of otherwise processed, and against all other unlawful forms of Processing.

2. NATURE OF PROCESSING

2.1 The Parties hereby acknowledge and agree that the following is an accurate description of the

Processing of data to be carried out by the Parties:-

Subject matter and duration of Processing

[ ]

Nature and purpose of Processing

[ ]

Types of Personal Data to be processed

[ ]

Categories of Data Subject to whom Personal Data relates

[ ]

Obligations and rights of the Controller

[ ]

3. CONSIDERATION

3.1 In consideration of the Controller engaging the services of the Processor to process Personal Data on its behalf, the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement and ensure compliance with Data Protection Law and, in particular, process all Personal Data on behalf of the Controller only for the purposes of performing its obligations under this Agreement and in accordance with the written instructions given by the Controller from time to time, and shall not modify or amend Personal Data unless specifically authorised in writing by the Controller.

4. SECURITY OBLIGATIONS OF THE PROCESSOR

4.1 The Processor shall only process Personal Data on behalf of the Controller as expressly authorised in writing by the Controller.

4.2 The Processor shall take appropriate Technical and Organisational Security Measures as are required under its own National Law to protect Personal Data processed by the Processor on behalf of the Controller against unlawful forms of processing.

4.3 The Processor shall ensure that any system on which the Processor or any Approved Sub-Contractor holds Personal Data, including backup data, is secure and ensures complete data integrity in accordance with the data security requirements and with good industry practice.

The Processor, as a minimum requirement, shall give due consideration to the following types of security measures:

Encryption and pseudonymisation;
Penetration testing;
Information Security Management Systems;
Physical Security;
Access Control;
Security and Privacy Enhancing Technologies;
Awareness, training and security checks in relation to personnel;

Incident/Response Management/Business Continuity; and
Audit Controls/Due Diligence.

5. CONFIDENTIALITY

5.1 The Processor shall maintain the Personal Data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor shall, save with the prior written consent of the Controller, not disclose any Personal Data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

5.2 The Processor shall not make any use of any Personal Data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

5.3 Nothing in this Agreement shall prevent either party from complying with any legal obligation imposed on it by a regulator or court. The parties shall, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of Personal Data.

6. PROCESSOR OBLIGATIONS

6.1 The Processor shall:-

6.1.1 only process or otherwise transfer Personal Data in or to any country outwith the European Economic or international organisation Area with the Controller's prior written consent and where both a data transfer risk assessment has been carried out and the appropriate EU model clauses have been completed and signed by the appropriate parties prior to any such data transfer taking place;

6.1.2 inform the Controller immediately if, in its opinion, an instruction from the Controller infringes any obligation under Data Protection Law.

6.1.3 maintain written records, including in electronic form, of all Processing activities carried out in performance of the Services or otherwise on behalf of the Controller containing the information set out in Article 30(2) of the General Directive on Data Protection 2016/679 ("GDPR").

6.1.4 provide the Controller with details of the Processor's Data Protection Officer or other designated individual with responsibility for data protection.

6.1.5 ensure that all Processor personnel receive adequate training on the Data Protection Law and in the care and handling of Personal Data;

6.1.6 unless prohibited by law, notify the Controller immediately (and in any event within 24 hours of becoming aware of same) if it considers, in its opinion (acting reasonably), that it is required by law to act other than in accordance with the instructions of the Controller;

6.1.7 promptly deal with any enquiry from the Controller or any of its affiliates which relate to the Processing of Personal Data by the Processor or by approved Sub-Contractors;

6.1.8 procure that only those authorised to process Personal Data on behalf of the Processor and approved Sub-Contractors that need to have access to Personal Data are granted access to such Personal Data;

6.1.9 take all reasonable steps to ensure the reliability and integrity of anyone who is authorised by the Processor who shall have access to the Personal Data and shall

ensure that any Processor personnel and approved Sub-Contractors who have access to such Personal Data shall comply with the provisions of Data Protection Law and this Agreement, and that appropriate statutory duties of confidentiality exist or appropriate contractually binding confidentiality undertakings have been entered into with those authorised by the Processor who have access to Personal Data and Sub-Contractors which are no less onerous than those set out in this Agreement;

6.1.10 notify the Controller of any actual or suspected Personal Data Breach including any unauthorised or accidental disclosure, loss, alteration unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed made by the Processor or Approved Sub-Contractors, immediately on becoming aware of such;

6.1.11 promptly provide to the Controller (and in any event within 24 hours) after any of the following events, all information in its possession concerning:- unauthorised or accidental disclosure of, or access to Personal Data made by Processor personnel or Approved Sub-Contractors; or any actual, suspected Personal Data breach or breach of Data Protection Law and following such a notification support the Controller to implement any measures necessary to restore the security of compromised Personal Data;

6.1.12 provide all reasonable assistance, including by such Technical and Organisational Measures as may be required by the Controller, to comply with its obligations concerning Personal Data including any subject access request and/or responding to any other data subject request made; reporting requirements for personal data breaches; data protection impact assessments or investigation or assessment of Processing initiated by the Information Commissioner in respect of Personal Data as soon as possible but in any event within 3 working days of receipt of the request by the Controller;

6.1.13 allow the Controller, its employees, auditors, authorised agents or advisers reasonable access to any relevant premises, during normal business hours, to inspect the procedures, measures and records referred to in this Agreement and contribute as is reasonable to those audits and inspections; and

6.1.14 notify the Controller within 2 working days if it or an approved Sub-contractor receives a data subject request or supervisory authority correspondence and forward same to the Controller. Any data subject request made to the Processor or approved Sub-contractor shall be dealt with by the Controller.

7. SUB-CONTRACTING

7.1 The Processor shall be permitted to appoint Sub-Contractors, and to disclose Personal Data to such Sub-Contractors for Processing in accordance with this Agreement provided always that:

7.1.1 the Processor provides the Controller with full details of the proposed Sub-contractor (including the results of the due diligence undertaken in accordance with this Agreement) before its appointment;

7.1.2 the Processor undertakes thorough due diligence on the proposed Sub-contractor, including a risk assessment of the information governance related practices and processes of the Sub-contractor, which will be used by the Processor to inform any decision on appointing the proposed Sub-contractor;

7.1.3 the sub-contract is on terms which are substantially the same as, but no less onerous than, the terms of this Agreement;

7.1.4 the Processor will immediately notify the Controller in the event that it becomes aware of any breach of Data Protection Law by any of the Approved Sub-Contractors in connection with this Agreement; and

7.1.5 the Sub-contractor's right to Process Personal Data terminates automatically on expiry or termination of the Contract for whatever reason.

7.2 The Processor shall comply with, and shall procure that its approved Sub-Contractors shall comply with the provisions of Data Protection Law in relation to all Personal Data that is Processed by it in connection with this Agreement.

7.3 The Processor shall obtain and maintain, and shall procure that its approved Sub-Contractors shall obtain and maintain, all necessary registrations and notifications that the Processor and each of the approved Sub-Contractors is obliged to obtain and maintain in accordance with Data Protection Law in respect of providing the Services.

7.4 The Processor shall not, and shall procure that any approved Sub-Contractor and Processor personnel shall not, disclose any Personal Data to any third party (including for the avoidance of doubt the Data Subject but excluding any approved Sub-Contractor), in any circumstances other than at the Controller's specific written request, or where required to do so by law (provided that the Processor shall use reasonable endeavours to notify the Controller in advance of such disclosure or immediately thereafter, unless prohibited by law).

7.5 The Processor shall procure that any approved Sub-Contractor takes such Technical and Organisational Security Measures as are required under its own National Law to protect Personal Data processed by the Processor on behalf of the Controller against unlawful forms of processing.

7.6 For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub-processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement and the Processor shall remain liable for the acts or omissions of its agents and approved Sub-Contractors in relation to Personal Data Processed under this Agreement.

7.7 The Processor shall inform the Controller in writing of any intended changes regarding any Sub-contractor and give the Controller no less than 5 working days to object to same.

8. TERM AND TERMINATION

8.1 This Agreement shall continue in full force and effect for so long as the Processor is Processing Personal Data on behalf of the Controller under the terms of the Contract.

8.2 This Agreement shall terminate automatically on termination of the Contract between the Controller and the Processor

8.3 On termination of this Agreement, the Processor shall promptly (and in any event within 5 working days of termination) cease Processing the Personal Data (whether provided by the Controller or which are derived from Personal Data provided by the Controller) and permanently and securely destroy the Personal Data so that it is no longer retrievable [*and/or deliver to the Controller all Personal Data together with all copies in any form and in any media in the Processor's power, possession or control*]. The Processor shall provide such information as is necessary to enable the Controller to satisfy itself of the Processor's compliance with this clause.

9. INDEMNITY

9.1 To such extent as arising as a result of a breach by the Processor (or its Sub-contractors) of this Agreement; or their respective obligations under data protection law; or any fault or

negligence of the Processor or its Sub-contractors, the Processor shall indemnify on demand and keep indemnified the Controller from and against:

9.1.1 any monetary penalties or fines levied by any relevant supervisory authority on the Controller;

9.1.2 the costs of an investigative, corrective or compensatory action required by any relevant supervisory authority, or of defending a proposed or actual enforcement taken by any relevant supervisory authority; and

9.1.3 any loss, damage or expense suffered or incurred by, awarded against or agreed to be paid by the Controller pursuant to a claim, action or challenge made by a third party (including by a Data Subject) against the Controller.

10. GOVERNING LAW

10.1 This Agreement shall be governed by and construed in accordance with the law of Scotland and the Scottish Courts shall have exclusive jurisdiction in respect of any dispute or claim arising out of or in connection with it or its subject matter or formation.

IN WITNESS WHEREOF this Agreement is signed on behalf of each of the parties by its duly authorised representative as follows:-

_____	_____
WITNESS SIGNATURE	AUDIT SCOTLAND
_____	_____
WITNESS FULL NAME	DATE
_____	_____
ADDRESS	PLACE OF SIGNING
_____	
_____	_____
WITNESS SIGNATURE	[PROCESSOR]
_____	_____
WITNESS FULL NAME	DATE
_____	_____
ADDRESS	PLACE OF SIGNING
_____	