SCHEDULE 3

DATA PROTECTION CLAUSES

The following definitions shall be included in Clause 1 (Definitions and Interpretation) in place of (where already contained) or in addition to (in the relevant alphabetical position) the definitions already contained in Clause 1 (Definitions and Interpretation):

[Service Provider][Contractor] shall be deemed to be included as applicable in the terminology currently included in the Contract.

"Controller" shall have the same meaning as in the Data Protection Legislation;

"[Contractor][Service Provider] Personnel" means all directors, officers, employees, agents, consultants and contractors of the [Service Provider][Contractor] and/or of any Sub-Contractor engaged in the performance of its obligations under this Contract;

"Data Loss Event" means any event that results, or may result, in unauthorised access to Personal Data held by the [Service Provider][Contractor] under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;

"Data Protection Legislation" means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;

"Data Protection Impact Assessment" means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

"Data Protection Officer" shall have the same meaning as in the Data Protection Legislation;

"Data Subject" shall have the same meaning as in the Data Protection Legislation;

"Data Subject Access Request" means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

"DPA 2018" means Data Protection Act 2018;

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

"Law" means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 9178, bye-law, enforceable right within the meaning of Section 2 of the

European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the [Service Provider][Contractor] is bound to comply;

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

"Personal Data" shall have the same meaning as in the Data Protection Legislation;

"Personal Data Breach" shall have the same meaning as in the Data Protection Legislation;

"Processor" shall have the same meaning as in the Data Protection Legislation;

"Protective Measures" means appropriate technical and organisational measures in accordance with Article 32, which may include but not be limited to: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;

"Sub-processor" means any third party appointed to process Personal Data on behalf of the [Service Provider][Contractor] under this Contract;

The following clause will be included in place of the current clause headed Data Protection in the Contract. In the event that the clause in the contract, which deals with Data Protection, also deals with another subject matter, the following clause will replace the Data Protection provisions of that clause only.

1. DATA PROTECTION

1.1 The parties acknowledge that for the purposes of the Data Protection Legislation, the [Authority][Council][Client][Customer] is the Controller and the [Service Provider][Contractor] is the Processor. The only processing that the [Service Provider][Contractor] is authorised to do is listed in the Schedule by the [Authority][Council][Client][Customer]and may not be determined by the [Service Provider][Contractor].

1.2 The [Service Provider][Contractor] shall notify the [Authority] [Council][Client][Customer] immediately if it considers that any of the [Authority's] [Council's][Client's[Customer's] instructions infringe the Data Protection Legislation.

1.3 The [Service Provider][Contractor] shall provide all reasonable assistance to the [Authority][Council][Client][Customer] in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the [Authority][Council][Client][Customer] , include:

1.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;

1.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

1.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

1.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The [Service Provider][Contractor] shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

1.4.1 process that Personal Data only in accordance with the Schedule, unless the [Service Provider][Contractor] is required to do otherwise by Law. If it is so required the [Service Provider][Contractor] shall promptly notify the [Authority][Council][Client][Customer] before processing the Personal Data unless prohibited by Law;

1.4.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the [Authority][Council][Client][Customer] as appropriate to protect against a Data Loss Event having taken account of the:

1.4.2.1 nature of the data to be protected;

1.4.2.2 harm that might result from a Data Loss Event;

1.4.2.3 state of technological development; and

1.4.2.4 cost of implementing any measures;

1.4.3 ensure that :

1.4.3.1 the [Service Provider][Contractor] Personnel do not process Personal Data except in accordance with this Contract (and in particular the Schedule);

1.4.3.2 it takes all reasonable steps to ensure the reliability and integrity of any [Service Provider][Contractor] Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the [Service Provider][Contractor]'s duties under this Clause 1 (Data Protection);

(ii) are subject to appropriate confidentiality undertakings with the [Service Provider][Contractor] or any Sub-processor;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the [Authority][Council][Client][Customer] or as otherwise permitted by this Contract; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and

1.4.3.3 not transfer Personal Data outside of the European Economic Area unless the prior written consent of the [Authority] [Council][Client][Customer] has been obtained and the following conditions are fulfilled:

(i) the [Authority][Council][Client][Customer] or the [Service Provider][Contractor] has provided appropriate safeguards in relation to the transfer;

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

(iii) the [Service Provider][Contractor] complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(iv) the [Service Provider][Contractor] complies with any reasonable instructions notified to it in advance by the [Authority][Council][Client][Customer] with respect to the processing of the Personal Data;

1.4.3.4 at the written direction of the [Authority] [Council][Client][Customer], delete or return Personal Data (and any copies of it) to the [Authority][Council][Client][Customer] on termination of the Contract unless the [Service Provider][Contractor] is required by Law to retain the Personal Data.

1.5 Subject to Sub-Clause 1.6 below, the [Service Provider][Contractor] shall notify the [Authority][Council][Client][Customer] immediately if it:

1.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

1.5.2 receives a request to rectify, block or erase any Personal Data;

1.5.3 receives any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation;

1.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;

1.5.5 receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

1.5.6 becomes aware of a Data Loss Event.

1.6 The [Service Provider][Contractor]'s obligation to notify under Sub-Clause 1.5 above shall include the provision of further information to the [Authority] [Council][Client][Customer] in phases, as details become available.

1.7 Taking into account the nature of the processing, the [Service Provider][Contractor] shall provide the [Authority][Council][Client][Customer] with full assistance in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under Sub-Clause 1.5 above (and insofar as possible within the timescales reasonably required by the [Authority][Council][Client][Customer]) including by promptly providing:

1.7.1 the [Authority][Council][Client][Customer] with full details and copies of the complaint, communication or request;

1.7.2 such assistance as is reasonably requested by the [Authority] [Council][Client][Customer] to enable the [Authority] [Council][Client][Customer] to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

1.7.3 the [Authority][Council][Client][Customer], at its request, with any Personal Data it holds in relation to a Data Subject;

1.7.4 assistance as requested by the [Authority][Council][Client][Customer] following any Data Loss Event;

1.7.5 assistance as requested by the [Authority][Council][Client][Customer] with respect to any request from the Information Commissioner's Office, or any consultation by the [Authority][Council][Client][Customer] with the Information Commissioner's Office.

1. The [Service Provider][Contractor] shall maintain complete and accurate records and information to demonstrate its compliance with this Clause 1 (Data Protection). This requirement does not apply where the [Service Provider][Contractor] employs fewer than two hundred and fifty (250) staff, unless:

1.8.1 the [Authority][Council][Client][Customer] determines that the processing is not occasional;

1.8.2 the [Authority][Council][Client][Customer] determines that the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

1.8.3 the [Authority][Council][Client][Customer] determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The [Service Provider][Contractor] shall allow for audits of its Data Processing activity by the [Authority][Council][Client][Customer] or the [Authority's][Council's][Client's][Customer's] designated auditor.

1.10 The [Service Provider][Contractor] shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the [Service Provider][Contractor] must:

1.11.1 notify the [Authority][Council][Client][Customer] in writing of the intended Sub-processor and processing;

1.11.2 obtain the written consent of the [Authority][Council][Client][Customer];

1.11.3 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this Clause 1 (Data Protection)such that they apply to the Sub-processor; and

1.11.4 provide the [Authority][Council][Client][Customer] with such information regarding the Sub-processor as the [Authority][Council][Client][Customer] may reasonably require.

1.12 The [Service Provider][Contractor] shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The [Authority][Council][Client][Customer] may, at any time on not less than thirty (30) Working Days' notice, revise this Clause 1 (Data Protection) by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).

1.14 The parties agree to take account of any non-mandatory guidance issued by the Information Commissioner's Office. The [Authority][Council][Client][Customer] may on not less than thirty (30) Working Days' notice to the [Service Provider][Contractor] amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Officer.

The Schedule

Processing, Personal Data and Data Subjects

1. The [Service Provider][Contractor] shall comply with any further written instructions with respect to processing by the [Authority] [Council][Client][Customer] .

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*
Nature and purposes of the processing	*[Please 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 e.g.: 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), Authority's/ 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]*