**DATA PROTECTION APPENDIX**

1. DEFINITIONS
	1. The following words shall have the meanings given:

|  |  |
| --- | --- |
| **Data Protection Legislation** | (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; and (iii) all applicable Law about the Processing of Personal Data and privacy; |
| **DPA 2018** | Data Protection Act 2018; |
| **GDPR** | the General Data Protection Regulation *(Regulation (EU) 2016/679);* |
| **LED** | Law Enforcement Directive *(Directive (EU) 2016/680);* |
| **Shared Personal Data** | the Personal Data to be shared between the parties under this Contract. |

* 1. For the purposes of this Contract the terms Data Controller, Processor, Data Subject, Personal Data, Processing, Personal Data Breach, Subject Access Request and “appropriate technical and organisational measures” shall have the meanings prescribed under the Data Protection Legislation.
	2. All other terms in this Appendix shall have the meanings assigned to them in the Contract to which this is appended.
1. **DATA PROTECTION**
	1. It is agreed and acknowledged by the Parties that where the Provider Processes Personal Data in performance of the Provider’s obligations under this Contract, the Provider carries out such Processing as a Data Controller, and not as a Processor.
	2. It is agreed and acknowledged that the Council is the Data Controller for the Personal Data that it holds and shares with the Provider under this Contract.
	3. As Controllers in common the Council and the Provider agree to share and Process the Personal Data on the terms set out in this Appendix and the schedules to this Contract and the Parties will comply with all the requirements of the Data Protection Legislation throughout the duration of this Contract.
	4. The Parties agree that the sharing of Personal Data is necessary for the purposes of this Contract as defined in the Specification, namely: [insert detail as required] (“the Agreed Purpose”) and the Parties shall not Process Shared Personal Data other than for the Agreed Purpose.
	5. Each Party will Process all Personal Data as set out in the Schedule of Processing, Personal Data and Data Subjects below.
	6. Each Party will implement appropriate technical and organisational measures to
		1. prevent:
			1. unauthorised or unlawful Processing of the Shared Personal Data; and
			2. the accidental loss or destruction of, or damage to, the Shared Personal Data; and
		2. ensure a level of security appropriate to:
			1. the harm that might result from such unauthorised or unlawful Processing or accidental loss, destruction or damage; and
			2. the nature of the Shared Personal Data to be protected

in such a manner that all Processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of Data Subjects .

* 1. Each Party shall ensure that it has legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal Data.
	2. Each Party in sharing Personal Data with the other, shall ensure that it provides clear and sufficient information to the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will Process their Personal Data, the legal basis for such purposes and such other information as is required by Article 13 of the GDPR including, if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer.
	3. Each Party in receiving Personal Data from the other, undertakes to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will Process their Personal Data, the legal basis for such purposes and such other information as is required by Article 14 of the GDPR including, if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer.
	4. The Parties each agree to provide such assistance as is reasonably required to enable the other P**a**rty to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.
	5. Each Party is responsible for maintaining a record of individual requests for information from Data Subjects, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the Data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.
	6. Subject to any statutory or stated retention periods, the Parties shall not retain or Process Shared Personal Data for longer than is necessary to carry out the Agreed Purpose.
	7. Any Personal Data that has been shared with a Party shall, at the direction of the other, disclosing, Party be returned or destroyed in the following circumstances:
		1. on termination of the Contract;
		2. on expiry of the Term of the Contract;
		3. once Processing of the Shared Personal Data is no longer necessary for the Agreed Purpose for which it was originally shared;

unless required by law to continue to store such Personal Data

* 1. If a Party appoints a third party Processor to Process the Shared Personal Data it shall comply with Article 28 and Article 30 of the GDPR and shall remain liable to the other Party for any breach, non-performance or non-observance of this Appendix by such other Processor in the same way and to the same extent as if such breach, non-performance or non-observance had been committed by the appointing Party.
	2. A Party may not transfer Shared Personal Data to a third party located outside the EEA unless it;
		1. complies with the provisions of Articles 26 of the GDPR (in the event the third party is a joint Controller); and
		2. ensures that (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 of the GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 of the GDPR; or (iii) one of the derogations for specific situations in Article 49 of the GDPR applies to the transfer.
	3. It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and Process the Shared Personal Data in accordance with the technical and organisational security measures together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the Processing of Personal Data.
	4. Each Party shall each comply with its obligation to report a Personal Data Breach to the other without undue delay and (where applicable) Data Subjects under Article 33 of the GDPR. The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner, including providing details of the nature of such Personal Data Breach, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, together with details of the likely consequences of the Personal Data Breach, and the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects.
	5. In the event of a dispute or claim brought by a Data Subject concerning the Processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will co-operate with a view to settling them amicably in a timely fashion.
	6. Each Party undertakes to indemnify the other and hold the other harmless from any claims, proceedings, actions, damages, costs, fines, expenses and any other liabilities which may arise out of, or in consequence of a breach or purported breach of the Data Protection Legislation or the performance or non-performance by that Party of its obligations under this Contract in relation to the Data Protection Legislation, including loss of or damage to property, financial loss arising from any breach of the Data Protection Legislation, or any other loss which is caused directly or indirectly by any act or omission of the Party arising from any breach of the Data Protection Legislation.
	7. The provisions of this Appendix shall apply during the Term of this Contract and indefinitely after its expiry.

**Schedule of Processing, Personal Data and Data Subjects**

The Parties shall Process all Personal Data in accordance with the Contract and the details set out within 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: employment processing, statutory obligation, recruitment assessment etc]* |
| Type of Personal Data being processed | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]* |
| Categories of Data Subject | *[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]* |
| Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | *[Describe how long the data will be retained for, how it be returned or destroyed]* |