**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);* |

* 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 – Joint Controllers** 
   1. For the purposes of this Appendix 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. It is agreed and acknowledged by the Parties that where there is Personal Data to be Processed in performance of this Contract, the Parties are the Joint Controllers of that Personal Data.
   3. The Parties agree that the Processing of Personal Data is required for the purpose of [insert detail] (“the Agreed Purpose”) and the Parties shall not Process Personal Data other than for the Agreed Purpose.
   4. The Parties will each comply with all the requirements of the Data Protection Legislation and shall assist each other in so complying.
   5. In particular, but without limiting its general effect, under clause 2.3 each Party shall:
      1. consult with the other Party about any notices given to Data Subjects in relation to the Personal Data;
      2. promptly inform the other Party about the receipt of any Data Subject Access Request;
      3. provide the other Party with reasonable assistance in complying with any Data Subject Access Request;
      4. not disclose or release any Personal Data in response to a Data Subject Access Request without first consulting the other Party wherever possible;
      5. assist the other Party, at the cost of the other Party, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
      6. use compatible technology for the processing of Personal Data to ensure that there is no lack of accuracy resulting from Personal Data transfers;
      7. maintain complete and accurate records and information to demonstrate its compliance with this Appendix and allow for audits by the other Party or the other Party’s designated auditor; and
      8. provide the other Party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Legislation, including the joint training of relevant staff, the procedures to be followed in the event of a data security breach, and the regular review of the parties’ compliance with the Data Protection Legislation.
   6. Each Party will notify the other of any Personal Data Breach without undue delay and in any event not later than 24 hours after becoming aware of such Personal Data Breach.
   7. Whenever a Party notifies the other of a Personal Data Breach as aforesaid, that Party will provide such information as the may be reasonably required including the nature of such Data Protection Breach, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, and provide the details of the likely consequences of the Data Protection Breach, and the measures taken or proposed to be taken to address such Data Protection Breach including, where appropriate, measures to mitigate its possible adverse effects.
   8. It is agreed and acknowledged by the Parties that any transfer of the Personal Data by the one Party to the other upon the expiry or other termination of this Contract that is necessary for the exercise of statutory functions, shall be considered lawful under the Data Protection Legislation, and therefore the relevant Party will transfer such Personal Data as aforesaid using an appropriately secure means of transfer. The Party will delete any copy of such Personal Data unless required by law to continue to store such Personal Data.
   9. Each Party shall indemnify and keep indemnified the other Party in full from and against all 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 Provider arising from any breach of the Data Protection Legislation.
   10. 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]* |