**DATA PROCESSING DEED/AGREEMENT\***

Data Processing Deed/Agreement\* to satisfy XXX of the Data Protection Act 2018

and

Articles xxxxx of the General Data Protection Regulation

BETWEEN

[…. insert Organisation name….], of [.…insert address….]

(Hereinafter also known as the Data Controller)

AND

[…. insert Organisation name….], of [.…insert address….]

(Hereinafter also known as the Data Processor)

In support of

The Services and / or Use of Data as Described in the Attached Schedules

**THIS DEED/AGREEMENT\*** is made on the

XXXX day of XXXX 20XX

\* Delete as appropriate

**Part 1: Generic Standard GDPR Clauses**

**[STANDARD DEFINITIONS, WHICH MAY NEED AMENDING]**

**Party**: a Party to this Agreement

**Agreement**: this deed;

**Law**: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, 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, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

**Processor Personnel**: means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement

**GDPR CLAUSE DEFINITIONS:**

**Data Protection Legislation**: (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**: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

**Controller**, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer** take the meaning given in the GDPR.

**Data Loss Event**: any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

**Data Subject Request**: 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**: Data Protection Act 2018

**GDPR**: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

**Joint Controllers:** where two or more Controllers jointly determine the purposes and means of processing

**LED**: Law Enforcement Directive *(Directive (EU) 2016/680)*

**Protective Measures**: appropriate technical and organisational measures which may include: 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 including those outlined in Schedule [x] (Security).

**Sub-processor**: any third Party appointed to process Personal Data on behalf of that Processor related to this Agreement

1. **DATA PROTECTION**
   1. The Parties acknowledge that for the purposes of the Data Protection Legislation, [ORG A] is the Controller and [ORG B] is the Processor unless otherwise specified in Schedule [X]. The only processing that the Processor is authorised to do is listed in Schedule [X] by the Controller and may not be determined by the Processor.
   2. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
   3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
      1. a systematic description of the envisaged processing operations and the purpose of the processing;
      2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;
      3. an assessment of the risks to the rights and freedoms of Data Subjects; and
      4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   4. The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
      1. process that Personal Data only in accordance with Schedule [X], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
      2. ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
         1. nature of the data to be protected;
         2. harm that might result from a Data Loss Event;
         3. state of technological development; and
         4. cost of implementing any measures;
      3. ensure that :
         1. the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);
         2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
            1. are aware of and comply with the Processor’s duties under this clause;
            2. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
            3. 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 Controller or as otherwise permitted by this Agreement; and
            4. have undergone adequate training in the use, care, protection and handling of Personal Data; and
      4. 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:
         1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
         2. the Data Subject has enforceable rights and effective legal remedies;
         3. 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
         4. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
      5. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.
   5. Subject to clause 1.6, the Processor shall notify the Controller immediately if it:
      1. receives a Data Subject Request (or purported Data Subject Request);
      2. receives a request to rectify, block or erase any Personal Data;
      3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
      4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
      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
      6. becomes aware of a Data Loss Event.
   6. The Processor’s obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.
   7. Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
      1. the Controller with full details and copies of the complaint, communication or request;
      2. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
      3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
      4. assistance as requested by the Controller following any Data Loss Event;
      5. assistance as requested by the Controller with respect to any request from the Information Commissioner’s Office, or any consultation by the Controller with the Information Commissioner's Office.
   8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
      1. the Controller determines that the processing is not occasional;
      2. the Controller determines 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; or
      3. the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
   9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
   10. Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
   11. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:
       1. notify the Controller in writing of the intended Sub-processor and processing;
       2. obtain the written consent of the Controller;
       3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and
       4. provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
   12. The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.
   13. The Controller may, at any time on not less than 30 Working Days’ notice, revise this clause 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 Agreement).
   14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Controller may on not less than 30 Working Days’ notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner’s Office.
   15. Where the Parties include two or more Joint Controllers as identified in Schedule [X] in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] in replacement of Clauses 1.1-1.14 for the Personal Data under Joint Control.
2. **DISPUTE RESOLUTION**
   1. Both parties shall aim to resolve all disputes, differences and questions by means of co-operation and consultation. Should this fail, then the dispute resolutions process in the standard NHS Commissioning contract will be engaged – the conditions contained in GC8. Other terms of that contract will not be applicable in any way to this contract
3. **LIABILITY AND INDEMNITY**
   1. Without affecting its liability for breach of any of its obligations under the service Deed, the Data Processor shall indemnify the Data Controller in full for costs, losses, charges, expenses it suffers arising out of the Data Processor’s loss of the NHS Information or unauthorised or unlawful use of it whether arising in negligence or is otherwise a breach of this Data Processing Deed and including any fine imposed on the Data Controller by the Information Commissioner by way of civil monetary penalty.
4. **FREEDOM INFORMATION**
   1. The Data Processor acknowledges that the Data Controller is subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).
   2. In addition, the Data Controllers may be statutorily required to disclose further information about the contracted service or the Deed itself in response to a specific request under FOIA or EIR, in which case:
   3. The Data Processor shall provide the Data Controllers with all reasonable assistance and co-operation to enable the Data Controllers to comply with its obligations under FOIA or EIR.
   4. The Data Controllers shall consult the Data Processor regarding commercial or other confidentiality issues in relation to the Deed, however the final decision about disclosure of information or application of exemptions shall rest solely with the Data Processor.

**DATA PROCESSING DEED BETWEEN THE DATA CONTROLLER AND THE DATA PROCESSOR**

**On behalf of the Data Controller**

The Data Controller........ [INSERT ORGANISATION NAME].............................

Executed as a deed by (name of company) acting by [a director and its secretary] [two directors]

Signature of Director: Date……………

Name

Position………………………………..

Signature of [Secretary][Director]: Date……………

Name

Position

**On behalf of the Data Processor**

The Data Processor........ [INSERT ORGANISATION NAME]..............................

Executed as a deed by (name of company) acting by [a director and its secretary] [two directors]

Signature of Director: Date……………

Name

Position………………………………..

Signature of [Secretary][Director]: Date……………

Name

Position

**Part 2: Schedules of Processing, Personal Data and Data Subjects**

**Processing, Personal Data and Data Subjects**

These Schedules shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

* + 1. The contact details of the Controller’s Data Protection Officer are: **[Insert** Contact details]
    2. The contact details of the Processor’s Data Protection Officer are: **[Insert** Contact details]
    3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
    4. Any such further instructions shall be incorporated into this Schedule.

**Schedule 1 – XXXX**

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of the Controller and Processor | The Parties acknowledge that for the purposes of the Data Protection Legislation, [ORG A] is the Controller and [ORG B] is the Processor in accordance with Clause 1.1.  **Guidance:** You may need to vary this section where (in the rare case) [ORG A] and [ORG B] have a different relationship. For example where the Parties are Joint Controller of some Personal Data:  *“Notwithstanding Clause 1.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:*  ***[Insert*** *the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]*  *In respect of Personal Data under Joint Control, Clause 1.1-1.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead.”* |
| Subject matter of the processing | *[This should be a high level, short description of what the processing is about i.e. its subject matter of the agreement.*  *Example: The processing is needed in order to ensure that the Processor can effectively deliver the agreement to provide a service to members of the public. ]* |
| 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]* |

**Part 3: Schedule for Joint Controller Agreements (Schedule Y)**

**Schedule Y: Joint Controller Agreement**

**[Guidance:** insert only where Joint Controller applies in Schedule X]

In this schedule the Parties must outline each party’s responsibilities for:

* providing information to data subjects under [Article 13 and 14](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN) of the GDPR.
* responding to data subject requests under [Articles 15-22](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN) of the GDPR
* notifying the Information Commissioner (and data subjects) where necessary about data breaches
* maintaining records of processing under [Article 30](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN) of the GDPR
* carrying out any required Data Protection Impact Assessment
* The agreement must include a statement as to who is the point of contact for data subjects.

The essence of this relationship shall be published.

You may wish to incorporate some clauses equivalent to those specified in Clause 1.2-1.14.

You may also wish to include an additional clause apportioning liability between the parties arising out of data protection; of data that is jointly controlled.

Where there is a Joint Control relationship, but no controller to processor relationship under the agreement, this completed Schedule Y should be used instead of Clause 1.1-1.15.