Data Processing Agreement

1 DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor. The only Processing that the Supplier is authorised to do is listed in Schedule 2, Table A of this Protocol by the Authority and may not be determined by the Supplier.

1.2 The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

1.3 The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, 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 Supplier 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 Schedule 2, Table A of this Protocol, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority 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 as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

1.4.3 ensure that :

(i) the Supplier Personnel do not Process Personal Data except in accordance with this Contract (and in particular Schedule 2, Table A of this Protocol).

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Supplier's duties under this Protocol;

(B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(C) 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 or as otherwise permitted by this Contract; and

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

1.4.4 not transfer Personal Data outside of the UK or the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

(i) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the GDPR or Article 37 of the Law Enforcement Directive (Directive (EU) 2016/680)) as determined by the Authority;

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

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection (by means of an EC adequacy decision) to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Authority in meeting its obligations); and

(iv) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;

1.4.5 at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination or expiry of the Contract unless the Supplier is required by Law to retain the Personal Data and provide a certificate of destruction.

1.5 Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority 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 Supplier's obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.

1.7 Taking into account the nature of the Processing, the Supplier shall provide the Authority 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 of this Protocol (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

1.7.1 the Authority with full details and copies of the complaint, communication or request;

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

1.7.3 the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

1.7.4 assistance as requested by the Authority following any Data Loss Event;

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

1.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol to comply with Article 30 EU GDPR 'Records of processing activities'. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

1.8.1 the Authority determines that the Processing is not occasional;

1.8.2 the Authority 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; and

1.8.3 the Authority determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Supplier shall allow for audits of its Processing activity by the Authority or the Authority's designated auditor.

1.10 The Supplier 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 Supplier must:

1.11.1 notify the Authority in writing of the intended Sub-processor and Processing;

1.11.2 obtain the written consent of the Authority;

1.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and

1.11.4 provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

1.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Authority may, at any time on not less than 30 Business Days' notice, revise this Protocol 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 guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Business Days' notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Schedule 2, Table A above from the date at which such notice is treated as having been received by the Supplier in accordance with Clause 27.2 of Schedule 2 of the Contract.

1.16 Subject to Clauses 1.13, 1.14, and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorized representative of both Parties.

1 DATA PROTECTION PROTOCOL (GDPR Article 28(3))

1 Table A – Processing, Personal Data and Data Subjects

Description	**Details**
Subject matter of the processing	*The Provider will store Personal Data for the purpose of providing clinical communications on behalf of the Authority.*
Duration of the processing	*The Provider will store Personal Data on behalf of the Authority for the duration of the Contract between the Parties and of the individual.*
Nature and purposes of the processing	*The Provider will store Personal Data on behalf of the Authority for the nature of processing as detailed below:* ● *Collection – of information from data subjects* ● *Recording – this information for the purpose of processing* ● *Organisation - to organise appropriate resources ie staff rostering* ● *Structuring – to determine appropriate resources ie staffing levels* ● *Storage – of information from data subjects* ● *Alteration – to data eg following a periodic review* ● *Retrieval – of historical data eg for purposes of safeguarding, ombudsmen queries* ● *Consultation – use of data ie to drive efficiencies*

	• *Disclosure by transmission – sharing appropriate data by secure means* *The Provider will store Personal Data on behalf of the Authority for the purpose of processing as detailed below:* • *To deliver person centred health and/or care* • *To fulfil contractual obligations* • *To satisfy Audit / Regulatory requirements and inspections*
Type of Personal Data	***Person Confidential Data (Individual Identifiable)*** *A non-sensitive identifier, the disclosure of which is unlikely to cause damage or distress to an individual or third party (exemptions apply).* *Defined in the Data Protection Act as:* *Data relating to a living individual who can be identified;* *from those data (e.g. an employee's name), or* *from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (e.g. an employee's payroll number)* *For NHS common law duty of confidence purposes, Individual Identifiers / Person Confidential Data also applies to deceased patients.* *This information includes single items such as:* *Name* *Address (home or business)* *Postcode*

	NHS No *Email address* *Date of birth* *Payroll number* *Driving Licence [shows date of birth and first part of surname] and photograph* ***Sensitive Personal Data (Individual Identifiable)*** *Information, the disclosure of which, is likely to cause damage or distress to an individual or third party e.g.:* *Personal Data consisting of information as to:* *Racial / ethnic origin* *Political opinions* *Religious beliefs* *Trade union membership* *Physical or mental health* *Sexual life* *Criminal offences* *AND* *…for Information mapping purposes will include information which may lead to damage or distress (e.g. breach of privacy, financial loss) such as:* *Biometrics; DNA Profile, Fingerprints, Clinical Photographs (Images),* *Bank, Financial Or Credit Card Details* *Mother's Maiden Name*

	National Insurance Number *Tax, Benefit Or Pension Records* *Health, Adoption, Employment, School, Social Services, Housing Records* *Child Protection* *This is not an exhaustive list.*
Categories of Data Subject	*The Provider processes the following categories of Personal Data:* ● *Controllers customers/clients/service users* ● *Controllers staff*
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	*The Provider will process data for the term of the Contract and return all data (in a portable format) once the Contract has ended.* *OR* *The Provider will process data for the term of the Contract and retain all adult social care records (with standard retention periods) for 8 years from the end of care or client last seen. Review and if no longer needed destroy.*

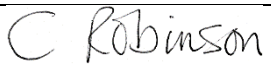
2 Definitions

The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract shall also apply to this Protocol. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

"**Data Loss Event**"	means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier 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 Impact Assessment**"	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"**Data Protection Officer**" and **"Data Subject**"	shall have the same meanings as set out in the GDPR;
"**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.
"**Personal Data Breach**"	shall have the same meaning as set out in the GDPR;
"**Protective Measures**"	means appropriate technical and organisational measures which may include: pseu donymising 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 such measures adopted by it;
"**Protocol**" or "**Data Protection Protocol**"	means this Data Protection Protocol;
"**Sub-processor**"	means any third party appointed to Process Personal Data on behalf of the Supplier related to this Contract.

Authorised Signatory

Wet Signatures are not required on the condition that the parties provide an unequivocal approval of terms email from the authorised signatory which will be appended to the final agreement.

Trust Service Lead	
Name	
Role	
Signature / Email Attached	
Date	
Trust Caldicott Guardian / Chief Clinical Information Officer	
Name	
Signature / Email Attached	
Date	
Data Processor Signatory	
Name	Claire Robinson
Role	Data Protection Officer
Signature / Email Attached	
Date	