SCHEDULE 8

DATA PROTECTION CLAUSE

1. Definitions

1.1

Applicable Laws: (a) European Union or Member State laws with respect to any Council Personal Data in respect of which the Council is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Council Personal Data in respect of which the Council is subject to any other Data Protection Laws;

Caldicott Guardian: the senior health professional responsible for safeguarding the confidentiality of patient information.

Caldicott Information Governance Review: the Information Governance Review (March 2013) also known as Caldicott 2, available at (https://www.gov.uk/government/publications/the-information-governance -review)

Caldicott Principles: the principles applying to the handling of patient-identifiable information set out in the report of the Caldicott Committee (1 December 1997)

Commission: has the meaning given to it in the GDPR;

Controller: has the meaning given to it in the GDPR;

Council: Cheshire East Borough Council;

Council Personal Data: any Personal Data Processed by a Contracted Processor on behalf of the Council pursuant to or in connection with this Contract;

Contracted Processor: the Provider or a Subprocessor;

Data Breach: has the meaning given to it in the Information Governance Review 2013.

Data Subject: has the meaning given to it in the GDPR;

Data Protection Laws: EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

Delete / Deletion: means deletion, removal of the Council Personal Data from the Provider's system using software certified to recognised international standards, including but not limited to, CESG HMG Infosec. Standard No: 5 Secure Sanitisation (Baseline and Enhanced);

European Economic Area: the European Economic Area (EEA) which consists of the European Union and all the European Free Trade Association (EFTA) countries except Switzerland.

EEA: the European Economic Area;

EU Data Protection Laws: EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

GDPR: EU General Data Protection Regulation EU 2016/679, as amended or re-enacted from time to time and any United Kingdom Act or European Union Regulation recognised in UK law substantially replacing the same.

Governing Body: in respect of any party, the board of directors, governing body, executive team or other body having overall responsibility for the actions of that party.

Information Governance Lead: an employee of the Provider who is responsible for information governance.

Member State: shall have the same meaning as set out in the GDPR.

National Institute for Health and Clinical Excellence or NICE: the special health authority responsible for providing national guidance on the promotion of good health and the prevention and treatment of ill health (or any successor body)

NHS Care Records Guarantee: the document setting out the rules that govern information held in the NHS Care Records Service, which is reviewed at least annually by the National Information Governance Board for Health and Social Care

NHS Information Governance Toolkit: an online system which allows NHS organisations and partners to assess themselves against Department of Health information governance policies and standards (https://www.igt.hscis.gov.uk/).

Personal Data: shall have the same meaning as set out in the GDPR.

Personal Data Breach: shall have the same meaning as set out in the GDPR.

Processing: shall have the same meaning as set out in the GDPR.

Processor: shall have the same meaning as set out in the GDPR.

Response to Caldicott: the Department of Health publication Information:To share or not to share? A Government response to the Caldicott Review September 2013, available at (https://www.gov.uk/government/publications/caldicott-information- governance-review-department-of-health-response)

Restricted Transfer:

i. a transfer of Council Personal Data from the Council to a Contracted Processor; or
ii. an onward transfer of Council Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

Senior Information Risk Owner: the Supplier's nominated person, being an executive or senior manager on the Governing Body of the Supplier, whose role it is to take ownership of the organisation's information risk policy, act as champion for information risk on the Governing Body of the Supplier and provide written advice to the accounting officer on the content of the organisation's statement of internal control in regard to information risk.

Services: the services and other activities to be supplied to or carried out by or on behalf of the Provider for the Council pursuant to this Contract;

Subprocessor: any person (including any third party, but excluding an employee of the Provider or any of its sub-contractors) appointed by or on behalf of the Provider to Process Personal Data on behalf of the Council in connection with this Contract; and

Supervisory Authority: shall have the same meaning as in the GDPR.

2. DATA SHARING AGREEMENTS

2.1 The Provider will enter into such data sharing agreements with the Council as it requires in such form as it requires and in accordance with any provisions set out in Schedule 2.

3. THE PROVIDER AS DATA CONTROLLER

3.1 The parties acknowledge that:

3.1.1 In relation to Personal Data processed by the Provider for the purpose of delivering the Services the Provider will be the sole Data Controller; and

3.1.2 In relation to Personal Data required by the Council for the purposes of quality assurance, performance management and contract management, that the Council and the Provider will be joint Data Controllers.

3.2 The Provider must ensure that all Personal Data processed by the Provider in the course of delivering the Services is processed in accordance with the relevant parties' joint obligations under the GDPR.

4. THE PROVIDER AS DATA PROCESSOR

4.1 Where the Provider, in the course of delivering the Services, acts as a Data Processor on behalf of the Council, the Provider must:

4.1.1 Process relevant Personal Data only to the extent necessary to perform its obligations under this Contract, and only in accordance with instructions given by the Council;

4.1.2 Take appropriate technical and organisational measures against any unauthorised or unlawful processing of that Personal Data, and against the accidental loss or destruction of or damage to such Personal Data having regard to the state of technological development, the nature of the data to be protected and the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

4.1.3 Take reasonable steps to ensure the reliability of Staff who will have access to Personal Data, and ensure that those Staff are aware of and trained in the policies and procedure identified in clause 3.2; and

4.2 Not cause or allow Personal Data to be transferred outside the EEA.

4.3 Data processed by the Provider in the course of delivering the Services include:

4.3.1 Publishing, maintaining and operating policies relating to confidentiality, data protection and information disclosures that comply with the Law, the Caldicott Principles and Good Clinical Practice;

4.3.2 Publishing, maintaining and operating policies that describe the personal responsibilities of Staff for handling Personal Data and applying those policies conscientiously;

4.3.3 Publishing, maintaining and operating a policy that supports the Provider's obligations under the NHS Care Records Guarantee;

4.3.4 Publishing, maintaining and operating agreed protocols to govern the disclosure of Personal Data;

4.3.5 Where appropriate having a system in place and a policy in relation to the recording of any telephone calls or other telehealth consultations in relation to the Services, including the retention and disposal of those recordings.

4.4 The Provider must have in place a communications strategy and implementation plan to ensure that Service Users are provided with, or have made readily available to them, the information specified in article 13(1) of the GDPR.

4.5 Where the Council requires information for the purposes of quality management, the Provider must provide anonymised, pseudonymised or aggregated data, and must not disclose that Personal Data to the Council for those purposes without written consent or some other lawful basis for disclosure.

4.6 The Provider must (unless it can lawfully justify non-disclosure) disclose defined or specified confidential patient information to or at the request of the Council where support has been provided under the s251 Regulations, respecting any individual Service User's objections and complying with other conditions of the relevant approval.

5. INFORMATION GOVERNANCE

5.1 The Provider must complete and publish an annual information governance assessment using the NHS Information Governance Toolkit.

5.2 The Provider must

(a) nominate an Information Governance Lead, to be responsible for information governance and for providing the Provider's Governing Body with regular reports on information governance matters, including details of all incidents of data loss and breach of confidence;

(b) nominate a Caldicott Guardian and a Senior Information Risk Owner, each of whom must be a member of the Provider's Governing Body;

(c) ensure that the Council is kept informed at all times of the identities of the Information Governance Lead, Caldicott Guardian and the Senior Information Risk Owner.

5.3 The Provider must adopt and implement the recommendations of the Caldicott Information Governance Review and the Response to Caldicott.

5.4 The Provider must, at least once in each Contract Year, audit its practices against quality requirements regarding data sharing set out in NICE Clinical Guideline 138.

5.5 The Provider must achieve a minimum level 2 performance against all requirements in the relevant NHS Information Governance Toolkit.

5.6 The Provider must report and publish any Data Breach and any Information Governance Breach in accordance with IG Guidance for Serious Incidents.

6. RESPONSIBILITIES WHEN ENGAGING SUB-CONTRACTORS

6.1 Subject to Schedule 1, clause 29 (Sub-Contracting) , if the Provider is to require any Sub-Contractor to process Personal Data on its behalf, the Provider must

6.1.1 Require that the Sub-Contractor provide sufficient guarantees in respect of its technical and organisational security measures governing the data processing to be carried out, and take reasonable steps to ensure compliance with those measures;

6.1.2 Ensure that the Sub-Contractor is engaged under the terms of a written agreement requiring the Sub-Contractor to

6.1.2.1 Process such Personal Data only in accordance with the Provider's instructions;

6.1.2.2 implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR;

6.1.2.3 Allow rights or audit and inspection in respect of relevant data handling systems to the Provider or the Council or any person authorised to act on their behalf;

6.1.2.4 Impose on its own Sub-Contractors (in the event the Sub-Contractor further sub-contracts any of its obligations) obligations that are substantially equivalent to the obligations imposed on the Sub-contractor by this Schedule 8.

7. PROCESSING OF PERSONAL DATA

7.1 The Provider warrants and represents that, before any Subprocessor, Processes any Council Personal Data on behalf of the Council, the Provider shall enter into an agreement with the Subprocessor that is compliant with Applicable Laws for the Processing of any Council Personal Data.

7.2 The Provider shall:

7.2.1 comply with all applicable Data Protection Laws in the Processing of Council Personal Data;

7.2.2 not Process Council Personal Data other than on the Council's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Provider shall to the extent permitted by Applicable Laws inform the relevant Council of that legal requirement before the relevant Processing of that Personal Data; and

7.2.3 not make or permit any Subprocessor to make any Restricted Transfers.

7.3 The Provider will (and will instruct each Subprocessor) to Process Council Personal Data, as reasonably necessary for the provision of the Services pursuant to this Contract.

7.4 Annex 1 to this Schedule 8 sets out certain information regarding the Contracted Processors' Processing of Council Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). The Council may make reasonable amendments to Annex 1 by written notice to the Provider from time to time as the Council reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this Contract) confers any right or imposes any obligation on any party to this Contract.

7.5 The Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Council Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Council Personal Data, as strictly necessary for the purposes of this Contract, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

7.6 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Provider shall in relation to Council Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

7.7 In assessing the appropriate level of security, the Provider shall in particular take account of the risks that are presented by Processing, in particular from a Personal Data Breach.

7.8 The Provider will appoint (and require that each Subprocessor appoints) Subprocessors in accordance with this Schedule.

7.9 The Provider may continue to use those Subprocessors already engaged by the Provider as at the date of this Framework Agreement, subject to the Provider in each case as soon as practicable meeting the obligations set out in clause 7.5.

7.10 The Provider shall give the Council prior written notice of the proposed appointment of each Subprocessor and, where appropriate during the Contract Term, each new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Provider shall not appoint (nor disclose any Council Personal Data to) the proposed Subprocessor except with the prior written consent of the Council.

7.11 With respect to each Subprocessor, the Provider shall:

7.11.1 before the Subprocessor first Processes Council Personal Data carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Council Personal Data required by this Contract;

7.11.2 ensure that the arrangement between the Provider, and the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Council Personal Data as those set out in this Contract and meet the requirements of article 28(3) of the GDPR;

7.11.3 ensure that the Subprocessor shall not make a Restricted Transfer of any Council Personal Data; and

7.11.4 provide to the Council for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Contract) as the Council may request from time to time.

7.12 The Provider shall ensure that each Subprocessor performs the obligations under this Schedule, as they apply to Processing of Council Personal Data carried out by that Subprocessor, as if it were party to this Contract in place of the Provider.

7.13 Taking into account the nature of the Processing, the Provider shall assist the Council by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Council's obligations, as reasonably understood by the Council, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.14 The Provider shall:

7.14.1 promptly notify the Council if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Council Personal Data; and

7.14.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Council or as required by Applicable Laws to which the Contracted Processor is subject, in which case the Provider shall to the extent permitted by Applicable Laws inform the Council of that legal requirement before the Contracted Processor responds to the request.

7.15 The Provider shall notify the Council without undue delay upon the Provider or any Subprocessor becoming aware of a Personal Data Breach affecting Council Personal Data, providing the Council with sufficient information to allow the Council to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.16 The Provider shall co-operate with the Council and take such reasonable commercial steps as are directed by the Council to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.17 The Provider shall provide reasonable assistance to the Council with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Council reasonably considers to be required of the Council by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Council Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

7.18 Subject to clauses 7.19 and 7.20 the Provider shall promptly and in any event within 30 days of the date of cessation of any Services involving the Processing of Council Personal Data (the "Cessation Date"), Delete and procure the Deletion of all copies of those Council Personal Data.

7.19 Subject to clause 7.20, the Council may in its absolute discretion by written notice to the Provider within 30 of the Cessation Date require the Provider to (a) return a complete copy of all Council Personal Data to the Council by secure file transfer in such format as is reasonably notified by the Council to the Provider; and (b) Delete and procure the Deletion of all other copies of Council Personal Data Processed by any Contracted Processor. the Provider shall comply with any such written request within 30 days of the Cessation Date.

7.20 Each Contracted Processor may retain Council Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Provider shall ensure the confidentiality of all such Council Personal Data and shall ensure that such Council Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

7.21 The Provider shall provide written certification to the Council that it has fully complied with this clause 7 within 30 days of the Cessation Date.

7.22 The Provider shall make available to the Council on request all information necessary to demonstrate compliance with this Contract, and shall allow for and contribute to audits, including inspections, by the Council or an auditor mandated by the Council in relation to the Processing of Council Personal Data by the Contracted Processors.

7.23 Information and audit rights of the Council only arise under clause 7.22 to the extent that this Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

7.24 The Council when undertaking an audit shall give the Provider reasonable notice of any audit or inspection to be conducted under clause 7.22 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment,

personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

7.24.1 to any individual unless he or she produces reasonable evidence of identity and authority;

7.24.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Council undertaking an audit has given notice to the Provider that this is the case before attendance outside those hours begins; or

7.24.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

7.24.3.1 the Council when undertaking an audit reasonably considers necessary because of genuine concerns as to the Provider's compliance with this Contract; or

7.24.3.2 the Council is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where the Council when undertaking an audit has identified its concerns or the relevant requirement or request in its notice to the Provider of the audit or inspection.

7.25 The parties acknowledge that nothing in this Agreement relieves the Processor of its own direct responsibilities and liabilities under the Data Protection Laws.

7.26 The Supplier will be liable for the following types of loss which will be regarded as direct and will be recoverable by the Council for any:

7.26.1 regulatory losses or fines arising directly from the Supplier’s breach of Data Protection Law; and

7.26.2 additional operational or administrative costs and expenses from any material breach of the Principal Agreement;

7.26.3 wasted expenditure or unnecessary charges the Council pays because of the Supplier’s default;

7.26.4 other liabilities suffered by the Council in connection with the loss of, corruption or damage to, or failure to deliver Council Data by the Supplier.

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Council Personal Data as required by Article 28(3) GDPR.

Contract Title	[Insert contract title here]
Subject matter and duration of the Processing of Council Personal Data	The subject matter and duration of the Processing of Council Personal Data are set out in this Agreement
The nature and purpose of the Processing of Council Personal Data	[Include description here] *[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.]*
The categories of Council Personal Data to be Processed	[Include list of data categories here] *[Examples include: Pension details, benefit details, disability details, ethnicity, employment history, bank details, annual leave details, pay details, qualifications, lifestyle information]*
The categories of Data Subject to whom Council Personal Data relates	[Include categories of data subjects here] *[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.]*
The obligations and rights of the Council	The obligations and rights of the Council are set out in this Agreement.