Dated:

Data Processing Agreement

Between

THE COUNTY COUNCIL OF THE CITY AND COUNTY OF CARDIFF
("Data Controller")

and

XXXXXXX

("Data Processor")

This Agreement is dated

PARTIES

(1) The County Council of the City and County of Cardiff whose principal offices are situated at County Hall, Atlantic Wharf, Cardiff, CF10 4UW (referred to as "the Local Authority" or "the Data Controller")

(2) XXXXXX incorporated and registered in England and Wales with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] ("the Processor" or "the Data Processor")

BACKGROUND

(A) The Data Controller and the Data Processor entered into an agreement dated 01/04/2019 that requires the Data Processor to process Personal Data on behalf of the Data Controller ("Services Agreement"].

(B) Under the terms of the Services Agreement the Data Processor will process Personal Data that is under the Data Controller's control. Such Personal Data is set out in Appendix 1 to this Agreement.

(C) This Agreement sets out the additional terms, requirements and conditions on which the Data Processor will process the Personal Data when providing services under the Services Agreement in order to ensure that both Parties are aware of and shall comply with their respective obligations under the Data Protection Legislation.

DEFINITIONS

The following definitions and rules of interpretation apply in this Agreement.

"Agreement" means this agreement, its schedules and any other documents attached to, or referred to as forming part of this agreement;

"Authorised Officer" means an officer nominated by the Local Authority;

"Commencement Date" means the commencement date set out in the Services Agreement.

“Data Subject” shall take the meaning given in the GDPR

“Data Processors System” means any system, including information technology systems owned or operated by the Data Processor from which the personal data is received in accordance with this Agreement

“**Data Protection Legislation”** means (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; (iii) all applicable Law about the processing of personal data and privacy.

“DPA 2018” means the Data Protection Act 2018

“GDPR” means the General Data Protection Regulation (Regulation (EU) 2016/679)

“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 Data Processor is bound to comply

“LED” means the Law Enforcement Directive (Directive (EU) 2016/680)

“Personal Data” shall take the meaning given in the GDPR and for the avoidance of doubt includes the personal data which is under the control of the Data Controller and which the Data Processor is or is required to process in connection with the provision of the services under the Services Agreement

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Security Breach” means any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

1 Security

1.1 The Data Processor must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security

measures set out in Appendix 1.

1.2 The Data Processor shall ensure that all Personal Data is kept secure and in an pseudonyised and encrypted form, and shall use appropriate security practices and systems applicable to the use of the Personal Data to prevent , and take prompt and proper remedial action against unauthorised access, copying, modification, storage, reproduction, display or distribution of the Personal Data. In particular,

1.3 The Data Processor shall:

i. Register their Organisation with the Information Commissioner, unless they are exempt from processing as defined by the Information Commissioner;

ii. keep all Personal Data strictly private and confidential;

iii. only disclose the Personal Data processed to third parties with the explicit consent of the Data Controller

iv. allow access to the Personal Data strictly on a 'need to know' basis and use appropriate access controls to ensure this requirement is satisfied;

v. ensure that any recipients of the Personal Data are subject to this binding duty of confidentiality in relation to the Personal Data. Personal Data must not be shared with any third party by the Data Processor unless the Local Authority has given prior written consent and instruction for this to take place.

vi. Ensure that any systems used to process the Personal Data have been appropriately tested to ensure the personal information stored is fully secure and protected.

vii. comply with the principles of the Data Protection Legislation when processing the Local Authority's information.

1.4 If either party becomes aware of any unauthorised or unlawful processing of Personal Data or that any Personal Data is lost or destroyed or has become damaged, corrupted or unusable that party shall, at its own expense, within 24 hours notify the other party and fully co-operate with the other party to remedy the issue as soon as reasonably practicable.

1.5 The Data Processor shall take reasonable precautions to preserve the integrity of any Personal Data processed by it and to prevent any corruption or loss of such Personal Data.

2 Personnel

2.1 The Data Processor will take steps to ensure the reliability of all of its personnel (whether employees or contractors) that may have access to the Personal Data and use all reasonable endeavors to ensure such persons have sufficient skills and training in the handling of Personal Data.

2.2 Without prejudice to the generality of clause 2.1, the Data Processor will ensure that all employees:-

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

© are aware both of the Data Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement are

2.3 Where required by the Data Protection Legislation, the Data Processor will ensure that it has a nominated Data Protection Officer.

2.4 The Data Processor will allow the Data Controller access to its records and/or provide evidence of compliance with clauses 2.1, 2.2 and 2.3 above as requested.

3 Purposes

3.1 The Data Controller and the Data Processor acknowledge that for the purpose of the Data Protection Legislation, the Data Controller is the controller and the Data Processor is the processor.

3.2 The Data Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Data Processor.

3.3 For the avoidance of any doubt, the Data Processor will act only in accordance with the Local Authority's instructions in relation to the Personal Data and will not use the Personal Data for any purpose other than to provide the services under the Services Agreement. The Data Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Data Processor must promptly notify the Data Controller if, in its opinion, the Data Controller's instruction would not comply with the Data Protection Legislation.

4 Subcontractors

4.1 The Data Processor is not permitted to subcontract any activity that will involve a third party processing the Personal Data without the Local Authority's prior written consent of the Local Authority.

4.2 Without prejudice to the generality of clause 4.1, the Data Processor shall only authorise a third party (subcontractor) to process the Personal Data if:

(a) the Data Controller provides prior written consent prior to the appointment of each subcontractor **OR** is provided with an opportunity to object to the appointment of each subcontractor within [seven 7) working] after the Data Processor supplies the Data Controller with full details regarding such subcontractor;

(b) the Data Processor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Data Controller's written request, provides the Data Controller with copies of such contracts;

(c) the Data Processor maintains control over all Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

4.3 Those subcontractors approved as at the commencement of this Agreement are as set out in Appendix 2. The Data Processor must list all approved subcontractors in Appendix 2 and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

4.4 Where the subcontractor fails to fulfil its obligations under such written agreement, the Data Processor remains fully liable to the Data Controller for the subcontractor's performance of its agreement obligations.

4.5 The Parties consider the Data Processor to control any Personal Data controlled by or in the possession of its subcontractors.

4.6 On the Data Controller's written request, the Data Processor will audit a subcontractor's compliance with its obligations regarding the Data Controller's Personal Data and provide the Data Controller with the audit results.

5 Transferring personal data outside the European Economic Area

5.1 The Data Processor shall not transfer or permit the transfer of Personal Data to any territory outside the European Economic Area without obtaining the Local Authority's prior written consent.

6 Providing Assistance

6.1 The Data Processor must , at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Data Controller as the Data Controller may reasonably require to enable the Data Controller to comply with:-

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation; and

© Freedom of Information requests which may be received from individuals whose Personal Data the Data Processor is processing on its behalf.

6.2 The Data Processor will promptly comply with any Data Controller request or instruction requiring the Data Processor to amend, transfer, delete or otherwise process any Personal Data or to stop, mitigate or remedy any unauthorised processing. .

6.3 The Data Processor will notify the Local Authority immediately of all communications and/or complaints the Data Processor receives from any person which suggests non-compliance with the Data Protection Legislation and the Data Processor will not do anything or enter into any communication about any such non-compliance unless the Local Authority expressly authorises the Data Processor to do so.

6.4 The Data Processor will provide the Local Authority with a copy of the Personal Data as soon as possible if they request the Data Processor to do so in the format and on the media which is specified in their request.

6.5 The Data Processor will promptly and, in any event within twenty four (24) hours without undue delay notify the Local Authority if it becomes aware of:

(a) any accidental, unauthorised or unlawful processing of the Personal Data; or

(b) any Personal Data Breach.

6.6 Where the Data Processor becomes aware of 6.5 (a) and/or 6.5 (b) above, it shall, without undue delay, also provide the Data Controller with the following information:

(a) description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;
(b) the likely consequences; and
(c) description of the measures taken, or proposed to be taken to address (a) and/or including measures to mitigate its possible adverse effects.

6.7 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Data Processor will reasonably co-operate with the Data Controller in the Data Controller's handling of the matter and to assist the Data Controller with meeting it's obligations under the Data Protection Legislation, including:

(a) assisting with any investigation;
(b) providing the Data Controller with physical access to any facilities and operations affected;
(c) facilitating interviews with the Data Processor's employees, former employees and others involved in the matter;
(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Data Controller; and
(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.8 The Data Processor will co-operate on request with the supervisory authority under Article 31 of the GDPR

6.9 At the Data Controller's request, the Data Processor will give the Data Controller a copy of or access to all or part of the Data Controller's Personal Data in its possession or control in the format and on the media reasonably specified by the Data Controller.

7 Audit

7.1 The Data Processor shall permit the Data Controller and its third party representatives to audit the Data Processor's compliance with its Agreement

obligations upon reasonable notice during the term of this Agreement and to provide the Local Authority with whatever information it needs to ensure both Parties are complying with their obligations under Article 28 of the GDPR.

7.2 The Data Processor shall give all necessary assistance to the conduct of such audits during the term of the Agreement including, but not limited to:

(a) physical access to, remote electronic access to, and copies of the records and any other information held at the Data Processor's premises or on systems storing Personal Data;

(b) access to and meetings with any of the Data Processor's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

8 Term and Termination

8.1 This Agreement shall commence on the Commencement Date. Unless terminated earlier in accordance with this clause, this Agreement shall automatically expire upon the termination, howsoever arising, of the Services Agreement]

8.2 The Local Authority will be entitled to terminate the Agreement immediately on written notice if the Data Processor is found to have breached the Data Protection Legislation, and/or the Data Processor's actions have led to the compromise of the Local Authority's Personal Data in any way and/or the Data Processor fails to comply with the terms of this Agreement..

8.3 This Agreement will terminate with immediate effect if the reason for ending the arrangement is because:

i. a resolution is passed or an order is made for the Data Processor to be wound up (other than for a solvent amalgamation or reconstruction);

ii. the Data Processor becomes subject to an administration order or a receiver or administrative receiver is appointed;

iii. somebody with a right to do so takes possession of any of the Data Processor's property or assets in the event of it being dissolved;

iv. the Data Processor ceases to carry on business in the United Kingdom.

8.4 Upon termination or expiry (for whatever reason) of this Agreement between the Local Authority and the Data Processor, the Data Processor will securely return and not retain all of the Local Authority's Personal Data in their possession relating to the delivery of this Agreement (unless the Local Authority directs in writing the Data Processor to securely destroy or delete such Personal Data) unless the provisions of clause 8.5 apply.

8.5 If any law, regulation, or government or regulatory body requires the Data Processor to retain any documents or materials that the Data Processor would otherwise be required to return or destroy, it will notify the Data Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

9 Transferring of this Agreement

9.1 The Data Processor shall not assign, sub-contract or in any other way dispose of the Agreement or any part of it without the Local Authority's prior written instruction.

10 Indemnity

10.1 The Data Processor agrees to indemnify and keep indemnified and defend at its own expense the Local Authority against all costs, claims, damages or expenses incurred by the Local Authority or for which the Local Authority may become liable due to any failure by the Data Processor or its employees or agents to comply with any of its obligation under this Agreement.

10.2 Any limitation of liability set out in the Services Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

10.3 The Data Processor shall take out insurance sufficient to cover any payment that may be required under Clause 10 and produce the policy and receipt for premium paid, to the Local Authorities on request.

11 Law

11.1 This Agreement is governed by and will be interpreted in accordance with the laws of England and Wales. In the event of a dispute between the parties, it is agreed that the courts of England and Wales will have exclusive jurisdiction to hear the case.

12 Third party rights

12.1 The Parties are entering into this arrangement for the benefit of the Parties and the individuals whose Personal Data the Data Processor will process each of whom will be entitled to enforce it. Other than that, no other person will have any enforceable rights under this arrangement and the Contracts (Rights of Third Parties) Act 1999 will not apply.

13 Retention of documents

13.1 The Data Processor will only store the Personal Data for the period of time as directed by the Local Authority. Once this specified time period ends, the Data Processor must contact the Data Controller and agree how the information will be securely returned to the Local Authority or, that the information can be securely destroyed. No information should be destroyed until this has been agreed by the Local Authority.

Signed for and on behalf of the Processor:

Signature: .....…

(authorised signatory)

Print name: .....

Position: ……

Date: .....……

Signed for and on behalf of the Local Authority:

Signature: .....…

(authorised signatory)

Print name: .....

Position: ……

Date: .....……

Appendix 1 – Personal Data

Personal Data that is being processed may include, but is not limited to the following. Please see the Service Specification for further detail in respect of Personal Data that is required to be held in relation to each individual:

- Name
- Date of birth
- Telephone Number
- Address
- Postcode
- Email Address
- Gender
- NHS No.
- Marital Status
- Driving Licence (if shows date of birth and first part of surname)
- Mother's Maiden Name
- Racial / Ethnic Origin
- Nationality
- Political Beliefs
- Religious Beliefs
- National Insurance Number
- Bank, Financial or credit card details
- Tax, benefit Records
- Adoption, employment, school, Social Services, housing records
- Child Protection
- Pensions Records
- Criminal Data e.g. offences
- Name, address, telephone number of next of kin, or any other person authorised to act on his/her behalf;

- Name, Address and Telephone Number of the guardian (If an individual is subject to guardianship)
- Name, address, telephone number of GP.
- Name, address and telephone number to the Social Work Team and any other professionals involved in the care and support of the individual
- Records requested by other professionals that inform the care and support plan and the positive behaviour support plans;
- Records relating to medical history, treatments, welfare and conduct, progress reports, educational needs/achievements and any other relevant information pertaining to significant events that has affected individuals.
- Completed accident forms.
- Date of commencement of the service.
- The contract between the Provider and the Individual specifying the agreed terms of their care and support.
- Date of termination of service.
- Record of the original care and support assessment of need.
- Date of Review/Reassessment of Service.
- Achieved outcomes for the individual's through the provision of support.
- Individual staff support schedules/work programme (as appropriate).
- Record of Hospital Admissions/Discharges
- Records of any complaints both formal and Informal made by an individual using the service or made by their NOK/representative, with a record of response/agreed actions Subject to MHA or MCA restrictions, including review and end dates.
- All accident/incident report forms affecting an Individual and written procedures to be followed in the event of an accident;
- Food record sheets;
- Handover documents that inform on duty support staff – to maintain consistency with service provision.
- Incident debriefing records
- Any written medication policies / procedures as appropriate to an individual's recorded needs, capacity/skill level.

- A record of all financial transactions undertaken
- All relevant assessments
- Care and Support Plan with agreed care outcomes;
- Any reviews of Care and Support Plans
- Risk assessments and risk management plans;
- Detail of all care provider, including daily records or records of specific care interventions
- Details of any identified changes in an individual's behaviour that is viewed as untoward or unusual.
- Medication records (if appropriate);
- Details of any special dietary needs and/or medical treatment required;
- Daily participation records that identify in detail the support activities and services provided that identify and confirm particular outcomes have been met and any new personal achievements made;
- Details of changes in an individual's personal circumstances, care and support needs or health condition.
- Correspondence, reports and records in relation to additional support provided by other partner organisations, including Children's Services

Appendix 2 – Sub-contractors

Appendix 2 – Subcontractor Information

Please complete one table per Subcontractor used:

Subcontractor Name:	
Address:	
Contact Name:	
Contact Phone Number:	
Email Address:	