Rossendale
BOROUGH COUNCIL

THE DATA PROCESSOR SUPPLEMENTAL AGREEMENT

RE: [INSERT SERVICE/PROJECT/CONTRACT NAME]

THIS AGREEMENT is made on the day of 2018

BETWEEN:

(1) ROSSENDALE BOROUGH COUNCIL The Business Centre, Futures Park, Bacup OL13 0BB (hereinafter called 'the Council') and

(2) [ ] Ltd a company registered in England and Wales (Company Number [ ]) and having its registered office at [ ] ("the Provider")

.

Whereas:

(1) The Council and the Provider have entered into a contract [dated [ ] [of even date herewith] pursuant to which the Provider is to deliver [ ] services to the Council for which the Council is the Data Controller ("the Contract").

(2) The Parties wish to enter into a data processing agreement that complies with the Data Protection Legislation

(3) This Agreement and the Schedules hereto set out the conditions on which the Provider shall obtain, store, share, transmit and dispose of Personal Data on behalf of the Council and the technical and organisational security controls the Provider shall deploy in order to safeguard Personal Data.

NOW IT IS AGREED as follows:

1. Definitions and Interpretation

1.1 In this Agreement, unless otherwise specified, the definitions and interpretation set out in Schedule 1 to this Agreement shall apply and all data protection terms shall be interpreted in accordance with the meaning ascribed to them in Data Protection Legislation

2. Consideration

2.1 In consideration of the payment of the sum of £1.00 the Council engage the services of the Provider, the Provider accepts the engagement to provide the service on the terms and conditions set out in in this Agreement.

3. Data Protection Notification

3.1 The Provider shall confirm in writing to the Council that, for the purposes of activities carried out by it as a Data Controller in its own right, it either has a valid Notification in the Register of Data Controllers as published by the Information Commissioner or is exempt from such Notification obligations.

4. Assignment and Subcontracting

4.1 Other than where explicitly provided for in the Contract, any rights, obligations and/or performance required under this Agreement shall not be assigned, novated or subcontracted to any Sub-Contractor or other third party without the prior written consent of the Council.

4.2 The Provider may only authorise a Sub-Contractor to process Personal Data subject to the Council's prior written consent and provided that the Contractor has supplied the Council with full details of such Sub-Contractor, including details of the location where it will process any Personal Data.

4.3 Before allowing any Sub-Contractor to process any Personal Data related to this Agreement, the Provider must:

(a) notify the Council in writing of the intended Sub-Contractor and Processing

(b) obtain the written consent of the Council;

(c) enter into a written agreement with the Sub-Contractor which give effect to the terms set out this Agreement such that they apply to the Sub-Contractor; and

(d) provide the Council with such information regarding the Sub-Contractor as the Council may reasonably require.

4.4 The Provider shall remain fully liable to the Council for the performance of any Subcontractor and all acts or omissions of any Sub-Contractor.

5. Not Used

6. Data Protection

6.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Council is the Controller and the Provider is the Processor. The only Processing that the Provider is authorised to do is listed in Schedule 2 by the Council and may not be determined by the Provider. The Provider shall comply with the Data Protection Legislation and all applicable law in the Processing of Personal Data and shall:

6.1.1 process Personal Data only to the extent and in such a manner as is necessary for the purposes specified in the Contract and this Agreement,

including the particulars outlined in Schedule 2 and in accordance with documented instructions issued by the Council from time to time and shall not process Personal Data for any other purpose unless required to do so by law.

6.1.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Council 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;

6.2 In carrying out Council instructions, the Provider shall comply with all documentation produced or agreed by the Council relating to the Processing of Personal Data in the delivery of the Contract.

6.3 The Provider acknowledges that where it does not process Personal Data in accordance with the Council's instructions but itself determines the purposes and means of Processing Personal Data it shall be considered to be a Data Controller in respect of that Processing.

6.4 The Provider may only delete, amend or transfer Personal Data as expressly authorised by the Council for the purposes specified in this Agreement and as set out in Schedule 2.

6.5 The Provider shall not delete, amend or transfer Personal Data in any circumstances other than as provided for under Clause 6.4 and under Clause 14 (Retention) without the express consent of the Council.

6.6 The Provider shall not transfer or facilitate the transfer of any Personal Data outside the UK or beyond the European Economic Area without the express written permission of the Council

6.7 The Provider shall comply with the Data Protection Legislation, in particular it shall:

6.7.1. maintain a written record of all Processing activities carried out on behalf of the Council, containing:

6.7.1.1 the parties' names and contact details and those of their representatives and data protection officers (where such officers are appointed);

6.7.1.2 the categories of Processing carried out on behalf of the Council;

6.7.1.3 where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards where relevant;

6.7.1.4 a general description of the Provider's technical and organisational security measures;

6.7.2 co-operate on request with the Information Commissioner's Office or any successor body functioning as a data protection supervisory authority; and

6.7.3 appoint a Data Protection Officer if required by Data Protection Legislation.

6.8 The Provider shall provide all reasonable assistance to the Council in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Council, include:

(a) a systematic description of the envisaged Processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6.9 The Provider shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement.

7. Provider Personnel

7.1 The Provider shall take all reasonable steps to ensure the reliability and integrity of all Provider Personnel who have access to Personal Data and shall ensure that it takes all reasonable steps to ensure the reliability and integrity of any Provider Personnel who have access to the Personal Data and ensure that they:

(a) are aware of and comply with the Provider's duties under this clause;

(b) are subject to appropriate confidentiality undertakings with the Provider or any Sub-Contractor;

(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 Council or as otherwise permitted by this Agreement; and

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

7.2 The Provider shall ensure that Provider Personnel :

7.2.1 receive information security training on induction and annual refresher training;

7.2.2 are aware of the controls the Provider has established for the protection of Personal Data at rest or in transit; in physical and electronic format, stored in both secure and non-secure locations

and of the Provider's procedure for the reporting and management of security incidents;

7.3 The Provider shall ensure that only such of the Provider Personnel who may assist in carrying out its obligations under this Agreement shall have access to Personal Data and that such Provider Personnel have been vetted in line with Good Industry Practice and in accordance with any specific requirements of the Council.

7.4 The Provider shall ensure that none of the Provider Personnel used to carry out the services disclose any Personal Data to any third party except where expressly authorised to do so for the delivery of the services and as specified in Schedule 2.

7.5 Save as provided in clause 7.4, the Provider shall ensure that none of the Provider Personnel publish, disclose or divulge any Personal Data to a third party unless instructed to do so in writing by the Council.

8. Technical and Organisational Measures

8.1 The information security regime implemented by the Provider shall be compliant with all relevant legislation, and shall conform to recognised Good Industry Practice.

8.2 Appropriate technical, security and organisational measures shall be taken by the Provider to safeguard against accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to, Personal Data.

8.3 The Provider shall apply organisational and technical controls such as network and system specific security, physical security, user access privileges, user passwords, including but not limited to the following to ensure that:

8.3.1 irrespective of whether Personal Data is at rest or in transit, the controls deployed are appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage taking account of the nature and sensitivity of Personal Data;

8.3.2 physical measures provide effective protection for information, systems and services from unauthorised access, theft, interference or damage;

8.3.3 procedures are in place to identify and resolve software and system faults and failures, including the identification of malicious software;

8.3.4 access to Personal Data is role based for legitimate business purposes in accordance with the "need to know" principle and that user permissions are controlled and granted and removed in line with job responsibilities;

8.3.5 sufficiently complex password controls are implemented for all authorised personnel with role based access to Personal Data;

8.3.6 passwords, usernames and access codes are not disclosed to any other person (whether employed by the Provider or not) and that all passwords and security codes are kept securely;

8.3.7 remote access to the Providers' secure network requires two factor authentication (something the user knows and a token they have);

8.3.8 where Personal Data is not stored solely on secure networks:

(i) only portable devices owned and controlled by the Provider are used to transport Personal Data and devices with built-in hard drives, deploy recognised industry standard encryption software;

(ii) only the minimum necessary Personal Data is transported on portable devices or in paper form

(iii) systems are in place to account for the movement of paper documents removed from and returned to the secure environment;

(iv) paper documents are kept secure and returned to the secure environment without delay and are not left in unattended vehicles; stored with portable devices or in portable device containers;

8.3.9 unencrypted email via the insecure internet is not used to communicate or transmit private, confidential or commercially sensitive Agreement Data;

8.3.10 exchanges of Personal Data shall conform with the secure methods for electronic transmission in any Information Sharing Agreements (ISAs) agreed by the Council with other parties;

8.3.11 all reasonable precautions are taken to preserve the integrity and prevent any corruption or loss, damage or destruction of Personal Data;

8.3.12 all reasonable steps are taken to maintain and audit compliance with above measures.

8.4 Within 20 Working Days after the Effective Date, the provider shall prepare and submit to the Council for approval a fully developed complete and up to date Security Management Plan providing a comprehensive written description of the technical and organisational methods employed to safeguard Personal Data supplementing any policies and procedures the Provider may have already supplied.

8.5 Except where the Provider's IT system security has been subject to penetration testing by an accredited provider in the 18 month period immediately prior to the date of this Agreement, the Provider shall arrange for such a test within the 6 month period immediately following the date of this Agreement. Where a test has taken place within the specified period, a summary of the findings, recommended remedial measures and the actual measures implemented by the Provider shall be supplied to the Council within 4 weeks from the date of this Agreement. In the event of a future test, the summary of the findings together with a plan of any measures the Provider intends to implement

shall be provided to the Council no later than 6 weeks after the Provider receives the Assessor's report.

8.6 In the event any Personal Data related to this Agreement in the possession of the Provider becomes lost, corrupted or rendered unusable for any reason, the Provider undertakes to promptly restore such Personal Data using its back up and/or disaster recovery procedures at no cost to the Council.

9. Security Incident Management, Reporting and Notification

9.1 The Provider shall operate an incident management procedure for the timely reporting, investigation and management of all security incidents.

9.2 A security incident is defined as:

9.2.1 a deliberate attempt, whether successful or not, to compromise Personal Data; or

9.2.2 accidental breach of privacy/confidentiality and/or the loss or theft of Personal Data, or

9.2.3 a breakdown in Provider systems/processes that has or potentially may lead to Personal Data becoming damaged or exposed to unauthorised sources.

9.3 In the event of a security incident which has the potential to compromise Personal Data or has compromised Personal Data, a senior officer designated by the Provider will be responsible for investigating the incident and for implementing any necessary urgent remedial measures to contain the incident and/or learn lessons to avoid a similar incident occurring.

9.4 The Provider's designated senior officer shall notify the Council's nominated representative no later than the next Working Day after the incident becomes known and will provide sufficient information to ensure

the Council is able to assess the nature and severity of the incident and the containment and recovery measures underway or planned.

9.5 The Provider shall co-operate with the Council's nominated representative on the management and resolution of all information security incidents.

9.6 The Provider accepts that the obligation as to whether or not it is necessary to notify the fact of a security incident to:

9.6.1 Data Subjects;

9.6.2 Data Controllers from whom Personal Data may have been sourced;

9.6.3 if appropriate, relevant regulatory bodies, is a decision for the Council and not the Provider.

9.7 Under no circumstances shall the Provider notify individuals or other bodies about a security incident unless expressly authorised to do so by the Council's nominated representative.

9.8 The Provider shall supply all information necessarily required by the Council in relation to security incidents on a timely basis to assist it in determining whether it is necessary to notify data subjects and/or other bodies and in dealing with any complaints, regulatory investigations and/or legal action brought against the Council.

10. Audit and Inspection

10.1 The Provider shall comply with all reasonable requests or directions from the Council for information necessary to satisfy itself that the Provider is in full compliance with its obligations under this Agreement and Data Protection Legislation and the Provider shall allow for and contribute to audits including access to the Provider's premises (upon the Council giving reasonable notice) for the purpose of inspecting all facilities,

systems, documents and electronic data relating to the Processing of Personal Data by the Provider and to audit Processing activities carried out by the Provider under this Agreement.

11. Data Protection related complaints and communications

11.1 The Provider shall notify the Council no later than the next Working Day following the receipt of any complaint, notice or communication from an individual, supervisory or government body:

11.1.1 relating directly or indirectly to the processing of Personal Data and/or

11.1.2 to the Council's statutory obligations under Data Protection Legislation, the common law duty of confidence or other privacy related legislation

11.2 The Provider shall provide the Council with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 12 (and insofar as possible within the timescales reasonably required by the Council) including by promptly providing:

(a) the Council with full details and copies of the complaint, communication or request;

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

(c) the Council, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Council following any Data Loss Event;

(e) assistance as requested by the Council with respect to any request from the Information Commissioner's Office, or any consultation by the Council with the Information Commissioner's Office.

11.3 The Provider shall immediately inform the Council if, in its opinion, a Council instruction infringes any Data Protection Legislation.

12. Subject Access Requests

12.1 Subject to clause 12.3, the Provider shall notify the Council immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) 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

(f) becomes aware of a Data Loss Event.

12.2 The Contractor's obligation to notify under clause 12.1 shall include the provision of further information to the Council in phases, as details become available.

12.3 The Provider acknowledges that the Council is responsible for responding to requests from individuals for access to their Personal Data and shall assist and cooperate with the Council in complying with its statutory obligations.

12.4 The Provider shall:

12.4.1 transfer the Subject Access Request to the Council as soon as practicable and in any event within three Working Days of receipt;

12.4.2 ensure that once in receipt or made aware that a Subject Access Request has been submitted, all the requested information is retained for potential disclosure;

12.4.3 provide the Council with a copy of all the Personal Data in its possession (including the sources of the information), in the form the Council requires within seven Working Days of receiving the request (or such shorter period as may be specified); and

12.4.4 provide all necessary assistance as reasonably requested to enable the Council to respond to the Subject Access Request within the time for compliance set out in Data Protection Legislation.

12.5 Under no circumstances shall the Provider respond directly to a Subject Access Request unless expressly authorised to do so in writing by the Council.

13. Freedom of Information

13.1 The Provider acknowledges that the Council is subject to the requirements of the Freedom of Information Act 2000 (FoIA) and the Environmental Information Regulations 2004 (EIRs) and shall assist and cooperate with the Council to enable it to comply with its Information disclosure obligations.

13.2 The Provider shall:

13.2.1 transfer to the Council all Requests for Information that it receives as soon as practicable and in any event within three Working Days of receiving a Request for Information;

13.2.2 ensure that once in receipt or made aware that a Request for Information has been submitted, all the requested Information is retained for potential disclosure;

13.2.3 provide the Council with a copy of all the Information in its possession relating to a Request for Information (including the sources of the information), in the form the Council requires within seven Working Days of receiving the Request for Information (or such shorter period as may be specified); and

13.2.4 provide all necessary assistance as reasonably requested to enable the Council to respond to the Request for Information within the time for compliance set out in Section 10 of the FoIA or Regulation 5 of the EIRs;

13.3 The Council shall be responsible for determining in its absolute discretion whether requested information is exempt from disclosure in accordance with the provisions of the FoIA, EIRs, or any other relevant statute or case law governing access to information.

13.4 Under no circumstances shall the Provider respond directly to a Request for Information unless expressly authorised to do so in writing by the Council.

13.5 The Provider acknowledges that the Council may be obliged under the FoIA or the EIRs to disclose information concerning the Provider or the Services:

13.5.1 in certain circumstances without consulting the Provider; or

13.5.2 following consultation with the Provider having taken its views into account;

13.5.3 provided always that the Council shall, in accordance with any recommendations in the Section 45 FoIA Code, take reasonable steps, where appropriate, to give the Provider prior notice, or failing that, to draw the disclosure to the Provider's attention after any such disclosure.

14. Retention

14.1 The Provider shall enter into a Disposal and Destruction Plan with the Council which will specify the requirements for the retention and disposal of Personal Data over the life of the Contract and on termination to ensure that Personal Data is not held longer than is necessary and that Personal Data is permanently and securely destroyed unless the Council instructs the Provider to transfer and/or supply Personal Data to the Council on termination or the Provider is required by law to retain Personal Data.

14.2 The Disposal and Destruction Plan shall be agreed no later than 3 months after the signing of this Agreement by both parties.

14.3 The implementation of the Disposal and Destruction Plan, including arrangements on termination shall be undertaken by the Provider at no cost to the Council.

15. Termination

15.1 This Agreement shall terminate automatically upon expiry or earlier termination of the Contract unless terminated earlier in accordance with Clause 15.2.

15.2 Without prejudice to any rights that have accrued under this Agreement or any of its rights or remedies, either party may terminate this Agreement by giving written notice to the other party if the other party

commits a material breach of any material term of this Agreement and if that breach is remediable fails to remedy that breach within a period of 30 days after being notified in writing to do so.

15.3 On termination of this Agreement for any reason, the Provider shall immediately cease processing of all Personal Data and at the Provider's expense in accordance with the Disposal and Destruction Plan shall either supply Personal Data to the Council in the format specified or arrange for it to be transferred as directed by the Council and shall ensure that all remaining copies of Personal Data, including residual Agreement Data, are permanently removed from the Provider's systems in so far as the Provider is not required by law to retain Personal Data.

15.4 The Provider shall provide written confirmation of compliance with clause 15.3 no later than 14 days after termination of this Agreement.

16. Variation

16.1 The Council may vary the terms of this Agreement subject to providing at least 20 Working Days' notice to take account of any guidance issued by the Information Commissioner's Office or otherwise.

16.2 Any other variations must be by mutual agreement

17. Indemnity

17.1 The Provider shall indemnify and keep indemnified the Council against all claims, losses, liabilities or costs (including legal fees and penalties) and expenses incurred by or awarded against the Council or for which the Council may become liable due to any failure by the Provider or the Provider Personnel to comply with any of its obligations under this Agreement or as a result of any negligence, or breach of Data Protection

Legislation, statute, common law or European law by the Provider in processing Personal Data.

18. Jurisdiction

18.1 This Agreement shall be governed by and construed in accordance with the law of England and Wales and the parties shall submit to the exclusive jurisdiction of the Courts of England and Wales.

IN WITNESS WHEREOF the parties hereto have executed this Agreement as a deed the day and year first before written

THE COMMON SEAL OF
ROSSENDALE BOROUGH COUNCIL
was hereunto affixed in the
presence of:

Authorised Signatory ……

Executed as a deed by

[ ]

Ltd acting by a director in the presence of:) ……

Director

Name: ……

Signature of Witness: ……

Name of Witness: ……

Address ……

……

Schedule 1

A) Definitions

“Personal Data”	means all Personal Data generated and obtained by the Data Processor in the delivery of the Contract
“the Contract”	The contract [dated [ ]] of even date herewith] under which the Provider provides the Services to the Council
“Data Impact Assessment”	means an assessment by the Data Controller of the impact of the envisaged processing on the protection of Personal Data.
“Data Controller” (including Joint Data Controller)	means as defined in Data Protection Legislation;
“Data Loss Event”	means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor 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 Processor”	means as defined in in Data Protection Legislation
“Data Protection Impact Assessment”	means an assessment by the Data Controller of the impact of the envisaged Processing on the protection of Personal Data.
“Data Protection Legislation”	i) unless and until the GDPR is no longer directly applicable in the UK, the GDPR, (ii) the DPA (iii) and any national implemented Laws, regulations and secondary legislation about the processing of personal data and privacy as amended or updated from time to time and (iv) any successor legislation to the GDPR or the DPA
“Data Protection Officer”	means as defined in Data Protection Legislation
“Data Subject”	means as defined in Data Protection Legislation
“DPA 2018”	means the Data Protection Act 2018
“Disposal and Destruction Plan”	means the Plan to be developed by the Council governing retention and disposal of Personal Data
“FOIA Code”	The Code of Practice issued by the Secretary of State pursuant to Section

	45 of the Freedom of Information Act 2000
“GDPR”	means the General Data Protection Regulation (Regulation (EU) 2016/679)
“Good Industry Practice”	means the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would reasonably and ordinarily expected at from time to time from of a skilled and experienced service provider engaged in a similar type of undertaking as that of the Provider as under the Contract under the same or similar circumstances
“Notification”	means registration as a Data Controller with the relevant national authority as defined in Data Protection Legislation
“Personal Data”	means as defined in in Data Protection Legislation
“Personal Data Breach”	means as defined in in Data Protection Legislation
Protective Measures:	means 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.
“Provider Personnel”	means all directors, officers, employees, agents, consultants and contractors of the Provider and/or of

	any subcontractor engaged in the performance of the Provider's obligations under this Agreement;
"Processing"	means as defined in in Data Protection Legislation
"Requests for Information"	A request for information pursuant to the Freedom of Information Act 2000 and/or a request for environmental information as defined in Regulation 2 of the Environmental Information Regulations 2004 (2004/3391)
"Security Management Plan"	means the Provider plan describing the technical and organisational measures for delivery of the services as designed, revised and implemented pursuant to clause 8.4
"Sensitive Personal Data"	Means data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) whether or not the a member of a trade union (e) physical or mental health or condition, (f) sexual life, (g) the commission or alleged commission of any offence, or (h) alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings. or such definition of sensitive or special category data as is provided for in Data Protection Legislation .
"the Services"	the services to be provided by the Provider under the Contract

“Special Categories of Personal Data”	means as defined in Article 9(1) of the GDPR
“Subject Access Request”	means a request by or on behalf of a Data Subject in accordance with the rights granted pursuant to the Data Protection Legislation to access their Personal Data
“Working Day”	A day other than a Saturday, Sunday or public holiday in England when banks in London are open for business

B) Interpretation

(i) Words importing one gender shall include any other gender, words importing the singular include the plural and vice versa and any reference to a person includes a reference to an individual, company, authority, board, association or any other body.

(ii) The headings for any Clause sub-Clause paragraph sub paragraph or Schedule are for ease of reference only and shall not be taken into account in the construction or interpretation of this Agreement and the parties agree to observe and perform all their respective covenants and obligations contained herein whether contained in any of the Clauses sub-Clauses paragraphs or sub-paragraphs or in any of the Schedules

(iii) The word “including” shall be construed so as not to limit the generality of any words or expressions with which it is used

(iv) Any covenant or obligation upon any party under this Agreement not to do an act or thing shall be deemed to include an obligation not to knowingly cause or suffer such act or thing to be done.

(v) Where any consent approval or other authorisation is required under this Agreement from either of the Parties it shall be implied (unless the contrary shall appear from the express terms of this Agreement) that the Party from which such consent approval or other authorisation is sought shall diligently and reasonably consider any written request therefore made by the other

Party and that such consent approval or other authorisation shall not be unreasonably withheld or delayed.

(vi) Any reference in this Agreement to a statute or order shall (unless stated to the contrary) include any statutory extension or modification of such statute or order and any regulations orders byelaws or other subordinate legislation already or hereafter to be made under or pursuant to it.

(vii) Reference in this Agreement to any Clause sub-Clause paragraph sub-paragraph or Schedule without further designation shall be construed as a reference to the Clause, sub-Clause, paragraph, sub-paragraph or Schedule to this Agreement so numbered.

(viii) The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes this Schedule.

Schedule 2
Schedule of Processing, Personal Data and Data Subjects

1. The Provider shall comply with any further written instructions with respect to processing by the Council.

2. Any such further instructions shall be incorporated into 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] - DESCRIBE WHO IS RESPONSIBLE (IF APPROPRIATE) FOR ISSUING/COMMUNICATING PRIVACY NOTICES, THE FORM

	THIS WILL TAKE AND HOW IT WILL BE DONE - DESCRIBE WHO IS RESPONSIBLE FOR GAINING CONSENT (IF APPROPRIATE) AND HOW THIS IS DONE - DESCRIBE WHO IS RESPONSIBLE FOR ACTING ON MARKETING PREFERENCES/OPT OUTS AND HOW THIS IS MANAGED/CONTROLLED - RECORD KEY CONTACT PERSONNEL AND CONTACT DETAILS FOR VARIOUS ACTIVITIES
Type of Personal Data	[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]