Template for Information Sharing or Processing Agreement

In relation to: [Project Name]

Between

St. Asaph City Council

And

[THIRD PARTY NAME]

This document is subject to [an annual review] by St. Asaph City Council

CONTENTS

THIS AGREEMENT is dated [DATE]

PARTIES

The Clerk of the St. Asaph City Council ('**The Data Controller**'); and.

[COMPLETE NAME AND ADDRESS OF THIRD PARTY] ('**The Data Processor**')

BACKGROUND

The **Data Controller** agrees to share the Personal Data with the **Data Processor** in the European Economic Area (EEA) on terms set out in the Agreement.

The **Data Processor** agrees to use the Personal Data within the EEA on the terms set out in this Agreement and in accordance with the Contract.

AGREED TERMS

1. INTERPRETATION

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

Definitions:

The Act: the Data Protection Act 1998, as amended from time to time.

Agreed Purpose: has the meaning given to it in *clause 2* of this Agreement.

The Agreement: this Agreement.

Business Day: a day other than a Saturday, Sunday or public holiday in England when banks in [London] are open for business.

The Contract: [COMPLETE]

The Contract Services: the services [the third party name] are contracted to deliver under [title of contract] entered into by ……………….. and [third party name] and dated [XXXXXX].

Data Protection Authority: the relevant data protection authority is The Information Commissioner, established under section 6 of the Data Protection Act 1998.

The Directive: EU Data Protection Directive (95/46/EC), as amended from time to time.

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

Data Sharing Code: the Information Commissioner's Data Sharing Code of Practice of May 2011.

The Parties: means ………………………. and [third party name].

Privacy and Data Protection Legislation: the Data Protection Act 1998, the Data Protection Directive (*95/46/EC*), the Electronic Communications Data Protection Directive (*2002/58/EC*), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2426/2003*) (as amended), the Human Rights Act 1998, the European Convention on Human Rights, as from 25 May 2018 the General Data Protection Regulation (EU 2016/679) and all applicable laws and regulations relating to the processing of the personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner, and the equivalent of any of the foregoing in any relevant jurisdiction. References to legislation include any amendments made to those laws from time to time.

The Personal Data: the personal data [and sensitive personal data] detailed in Schedule 2 and to be shared between the parties under *clause 5* of this Agreement.

Subject Access Request: has the same meaning as "Right of access to personal data" as in GDPR May 25th 2018

Term: [include the agreed length of the data sharing initiative]

Data Controller, **Data Processor**, **Data Subject, Personal Data**, **Sensitive Personal Data** and **Processing** shall have the meanings given to them in the Act.

Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

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 the schedules.

Unless the context otherwise, requires, words in the singular shall include the plural and in the plural shall include the singular.

A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

References to clauses and Schedules are to the clauses and Schedules of this agreement and references to paragraphs are to paragraphs of the relevant Schedule.

Commented [LS2]: Retain/delete as appropriate dependent on whether sensitive personal data is being processed. **Sensitive personal data** is personal data about an individual's, political opinions, religious beliefs, physical or mental health, sexual life, commission or alleged commission of criminal offences (and criminal proceedings relating to such an offence) and membership of trade unions. The GDPR 2018 imposes tighter restrictions on the processing of sensitive personal data which can be dealt with in Clause 5.

Commented [LS3]: Schedule 1 gives guidance on what is meant by personal data.

Commented [LS4]: Processing means almost anything you can do with personal data such as storing, disclosing, analysing and publishing etc.

Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

In the case of any ambiguity between any provision contained in the body of this agreement and any provision contained in the Schedules or appendices, the provision in the body of this agreement shall take precedence.

A reference to **writing** or **written** includes letter, fax and email.

Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.

2. COMPLIANCE WITH DATA PROTECTION LAWS

2.1 The **Parties** acknowledge that under **the Act**, GDPR May 25th 2018, is a [Data Controller] and [third party name] is a [Data Processor] where processing personal data under the terms of the **Agreement**. Each **Party** must ensure compliance with the **Privacy and Data Protection Legislation** at all times during the **Term** of **the Agreement**.

3. USE, DISCLOSURE AND PUBLICATION

3.1 The **Data Processor** agrees to process the **Personal Data**, as described in clause 5, only for the purposes outlined in clause 4 of the **Agreement** and strictly for no other purpose without the written authority of the **Data Controller**.

3.2 The **Data Processor** will NOT disclose or share the **Personal Data** processed under the **Agreement**, with any third party without the written authority of the **Data Controller.**

3.3 The **Data Processor** is prohibited from publishing, copying, transferring or duplicating any information without the written authority of the **Data Controller**.

4. PURPOSE

4.1 The **Agreement** sets out the framework for the sharing of **Personal Data** between the **Data Controller**. It sets out the purposes for which the **Personal data** may be processed by the

Commented [LS5]: A Data Controller is an organisation who determines the manner and purpose of the processing of personal data. A Data Processor is an organisation who processes personal data under the instruction of the Data Controller. A Data Controller is responsible for compliance with the GDPR May 25th 2018 and will be liable in respect of any breaches of that Act. A Data Controller cannot seek to sub-contract or assign its responsibility for compliance with the GDPR May 25th 2018 to a Data Processor.

Parties, the principles and procedures that the **Parties** shall adhere to, and the responsibilities the **Parties** owe to each other.

4.2 The **Parties** consider this data sharing initiative necessary in order for the Data Processor to deliver **the Contract Services**. Schedule 1 to the Agreement provides a detailed outline of the Contract Services and how the personal data will be processed to deliver those services.

4.3 The **Data Processor** agrees to only **process** the **Personal data** in accordance with the **Data Controller's** instructions, and only for the purposes of providing the **Contract Services** as described in Schedule 1. The **Parties** shall not process **Personal Data** in a way that is incompatible with the purposes described in this clause (the **Agreed Purpose**).

4.4 Each party shall appoint a single point of contact (SPoC) who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative. The points of contact for each of the parties are:

[Data Controller's SPoC –

[Data Processor's SPoC – Clerk ay St. Asaph City Council

Contact phone number:

5 PERSONAL DATA

5.1 The Personal Data processed under the Agreement will comprise of [please provide a high level description here]. A more detailed description of the volume, types and variables of Personal Data processed under **the Agreement** is set out in Schedule 2 to **the Agreement**.

5.2 **The Parties** agree that the **Personal Data** processed under the **Agreement** must not be irrelevant or excessive with regard to the Agreed Purposes set out in Clause 4.

6 FAIR AND LAWFUL PROCESSING

6.1 Each **Party** shall ensure that it processes the **Personal Data** fairly and lawfully in accordance **with the Privacy Legislation** during the **Term** of **the Agreement**. Further, the **Data Controller** shall ensure that the

processing satisfies an appropriate condition under Schedule 2 and where relevant Schedule 3 of the Act.

7 DATA ACCURACY

The **Data Processor** agrees to ensure that the **Personal Data** processed is accurate and kept up to date. The **Data Processor** agrees to review the accuracy of the personal data on their system(s) and make any necessary changes to any **Personal Data** which is inaccurate or requires updating.

8 DATA SUBJECTS' RIGHTS

8.1 **Data Subjects** have the rights in relation to their personal data under the Privacy Legislation. Those rights include ;
(i) The right to be informed
(ii) The right of access
(iii) The right to rectification
(iv) The right to erasure
(v) The right to restrict processing
(vi) The right to data portability
(vii) The right to object
(viii) Rights in relation to automated decision making and profiling

8.2 To facilitate the above rights, the **Data Processor** agrees to store or record the **Personal Data** processed under **the Agreement** in a structured, commonly used and machine readable form.

8.3 The **Data Processor** agrees to notify the **Data Controller** immediately and no later than 48 hours upon receipt by the **Data Processor** of a request from an individual seeking to exercise any of their rights under the **Privacy and Data Protection Legislation**, including those rights as described in clauses 8.1 above. The **Data Processor** agrees to notify the **Data Controller** immediately [and no later than 48 hours] upon receipt of any complaint from an individual regarding the processing of **Personal Data** under the **Agreement**. The **Data Processor** will provide the **Data Controller** with full co-operation and assistance in relation to any such complaint or request from an individual regarding the **Processing** of **Personal Data** under this **Agreement**.

8.4 The **Data Processor** agrees to act only under the **Data Controller's** instructions in relation to any activities undertaken to resolve any complaints or comply with any requests from individuals under clause 8.

8.5 The **Data Processor's** SPoC is required to maintain a record of requests or complaints from data subjects seeking to exercise their rights under the **Privacy and Data Protection Legislation**, including requests for **Personal Data** processed under this **Agreement**. The records described in this clause must include copies of the request for information or complaint, details of the data accessed and shared and where relevant, notes of any meeting, measures taken by the **Data Processor** to resolve the complaint, correspondence or phone calls relating to the request or complaint.

9 RECORD KEEPING

9.1 In addition to the record keeping obligations under clause 8.4, the **Data Processor** agrees to maintain records of all **Personal Data** processed under the **Agreement** and its processing activities. The **Data Controller** reserves the right to inspect the records maintained by the **Data Processor** under this clause and clause 8.4 at any time.

10 DATA RETENTION AND DELETION

10.1   The **Data Processor** shall not retain or process **Personal Data** for longer than is necessary to carry out the Agreed Purposes or for longer than any period set by the Data Controller. For the avoidance of doubt, t**he Data Controller** reserves the right to determine the periods for which the **Data Processor** may retain the **Personal Data** processed under this Agreement.

10.2 On the instructions of the **Data Controller**, the **Data Processor** shall ensure that the **Personal Data** processed under this Agreement are returned to the Data Controller or destroyed in accordance with the **Data Controller's** instructions. The **Data Controller** reserves the right to issue instructions to the **Data Processor** under this Clause at any time.

10.3The **Data Controller** reserves the right to issue instructions to the **Data Processor** as to the methods by which **Personal Data** is destroyed under clauses 10.1 and 10.2.

10.4Following the deletion of Personal Data under clause 10.1 and 10.2, the **Data Processor** shall notify the **Data Controller** that the **Personal Data** in question has been deleted. Where applicable, the **Data Processor** shall also provide confirmation that the **Personal Data** has been destroyed in accordance with any instructions issued by the **Data Controller** under clause 10.3.

11 THIRD PARTY ACCESS AND INTERNATIONAL TRANSFERS

11.1   For the purposes of this clause, international transfers of the **Personal Data** shall mean any sharing of **Personal Data** by the **Data Processor** with a third party, and shall include, but is not limited to, the following:

Storing the **Personal Data** on servers outside the EEA.

subcontracting the processing of **Personal Data** to data processors located outside the EEA.

granting third parties located outside the EEA access rights to the **Personal Data**.

11.2 The **Data Processor** shall not disclose or transfer the **Personal Data** to a third party without the prior written authorisation of the **Data Controller**. If the **Data Controller** authorises the disclosure of the **Personal Data** to a third party, the **Data Processor** agrees to enter into an information sharing agreement with any relevant third party which reflects the terms of the **Agreement**. The **Data Processor** agrees to provide the **Data Controller** with copies of any such information sharing agreement with a third party. The **Data Controller** reserves the right of approval of any such information sharing agreement and may request the **Data Processor** to make any amendments deemed necessary to such an agreement to ensure compliance with the **Privacy and Data Protection Legislation**.

11.3 The **Data Processor** shall not disclose or transfer the **Personal Data** to a third party located outside the EEA without the prior written authorisation of the **Data Controller.**

12 SECURITY AND TRAINING

12.1   The **Data Processor** agrees to implement appropriate technological and organisational measures to prevent;

unauthorised or unlawful processing of the **Personal Data**; and

the accidental loss or destruction of, or damage to, **the Personal Data**

ensure a level of security appropriate to:

the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

the nature of the **Personal Data** to be protected.

Commented [LS10]: Please note that if the personal data is transferred outside of the EEA then certain adequacy arrangements must be in place. Those arrangements can include using a specific set of contractual clauses which have been approved by the European Commission to govern the international transfer.

12.2 Specifically, the **Data Processor** agrees to implement the technological and organisational security measures described in Schedule 3. The **Data Processor** agrees to notify the **Data Controller** of any material change to the measures as described in Schedule 3.

12.3It is the responsibility of each **Party** to ensure that its staff members are appropriately trained to handle and process the Personal Data in accordance with the technical and organisational security measures set out in Schedule 3 together with any other applicable national data protection laws and guidance.

12.4The level, content and regularity of training referred to in clause 11.3 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and processing of the **Personal Data**.

13 FREEDOM OF INFORMATION

13.1   The **Data Processor** recognises that the **Data Controller** is a public authority for the purposes of the Freedom of Information Act 2000 and may be required to disclose information about **the Agreement**, the services provided by the **Data Processor** under **the Agreement** and the processing carried out under **the Agreement**. The **Data Processor** agrees to provide any reasonable assistance to the **Data Controller** as is necessary to enable the **Data Controller** to comply with its obligations under the Freedom of Information Act 2000.

14 DATA SECURITY BREACHES AND REPORTING PROCEDURES

14.1   The **Data Processor** is under a strict obligation to immediately notify the **Data Controller** of any **Data Security Breach** and no later than within 24 hours of the Data Processor becoming aware of the breach.

14.2 In the event of a **Data Security Breach**, the **Data Processor** is required to provide the **Data Controller** with the information detailed in Schedule 3.

14.3The **Data Processor** agrees to provide any reasonable assistance as is required by the **Data Controller** or the **Data Protection Authority** to facilitate the handling of any **Data Security breach** in an expeditious and compliant manner.

Commented [LS11]: Remember to be valid a FOI request does not have to expressly state that it is made under the Freedom of Information Act 2000. However, to be a valid FOI request must be in writing, state the name of the requester, an address for correspondence and describe the information the requester is seeking.

Commented [LS12]: Subject to further discussion with the Data Protection Officer.

15 REVIEW AND TERMINATION OF AGREEMENT

15.1 **The Parties** shall review the effectiveness of the processing of **Personal Data** under this Agreement every […] months. The **Data Controller** may continue, amend or terminate the **Agreement** depending on the outcome of this review.

15.2 The review described in clause 15.1 will involve:

Assessing whether the purposes for which the Personal Data is being processed are still the ones listed in clause 4 of the **Agreement**;

Assessing whether the **Personal Data** is still as listed in clause 6 of the Agreement;

Assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and

Assessing whether personal data breaches involving the **Personal Data** have been handled in accordance with **the Agreement** and the applicable legal framework.

Assessing whether the technical and organisational measures listed in Schedule 3 to the **Agreement** are still in place and are adequate to prevent unauthorised or unlawful processing and accidental loss or destruction of, or damage to, the **Personal Data**.

16 RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DATA PROTECTION AUTHORITY

16.1 In the event of a dispute or claim brought by a data subject or the **Data Protection Authority** concerning the processing of **Personal Data** against either or both parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

16.2 The **Parties** agree to respond to any generally available non-binding mediation procedure initiated by a **Data Subject** or by the **Data Protection Authority**. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

16.3 Each **Party** shall abide by a decision of a competent court of the **Data Controller's** country of establishment or of the **Data**

Protection Authority in the **Data Controller's** country of establishment (namely the Information Commissioner).

17 THIRD PARTY RIGHTS

17.1   Except as expressly provided in clause 8 (data subjects rights), a person who is not a party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

18 SEVERANCE

18.1   If any provision or part-provision of the **Agreement** is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this agreement.

18.2   If the **Data Controller** gives notice the **Data Processor** that any provision or part-provision of this agreement is invalid, illegal or unenforceable, the **Parties** shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended commercial result of the original provision.

19 CHANGES TO THE APPLICABLE LAW

19.1   In case the applicable data protection and ancillary laws change in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Data Controller reserves the right to amend the Agreement. In such circumstances, the **Data Processor** agrees to implement any changes to its processing activities as are necessary to comply with the amended terms of the **Agreement**.

20 NO PARTNERSHIP OR AGENCY

20.1   Nothing in **the Agreement** is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

21 ENTIRE AGREEMENT

21.1 **The Agreement** and **the Contract to the extent it applies to this Agreement** constitute the entire agreement between the **Parties** and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

21.2 Each **Party** acknowledges that in entering into the **Agreement it does not rely on, and shall have no remedies in respect** of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in the **Agreement**.

21.3 Each **Party** agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misrepresentation based on any statement in the **Agreement**.

22 FURTHER ASSURANCE

22.1 At its own expense, the **Data Processor** shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may be required for the purpose of giving full effect to this **Agreement**.

23 RIGHTS AND REMEDIES

23.1 The rights and remedies provided under the **Agreement** are in addition to, and not exclusive of, any rights or remedies provided by law.

24 NOTICE

24.1 Any notice or other communication given to a **Party** under or in connection with this agreement shall be in writing, addressed to the SPoCs and shall be:

delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); and

sent by email to the SPOC.

24.2 Any notice [or communication] shall be deemed to have been received:

if delivered by hand, on signature of a delivery receipt [or at the time the notice is left at the proper address];

if sent by pre-paid first-class post or other next working day delivery service, at [9.00 am] on the [second] Business Day after posting [or at the time recorded by the delivery service].

if sent by fax [or email], at [9.00 am] on the next Business Day after transmission.

24.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution

25 GOVERNING LAW

25.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

26.1 This agreement has been entered into on the date stated at the beginning of it.

Schedule 1 – The Contract Services

Please provide an outline of the services the contractor is providing and how the Data Processor will process personal data to deliver those services. Please ensure this description clearly identifies the various stages at which the personal data will pass between the contractor and the University.

Schedule 2 Description of Personal Data

Please outline the personal data which will be processed under this agreement. Specifically, please outline the specific individuals or group[/s] of individuals the personal data relates to, the type of personal data which will be processed (e.g. names, dates of birth, medical information] and the volume of personal data which will be processed

Personal data *means any data from which a living individual can be identified, either from that data alone or where the data is matched with other data. For example, personal data can include information about individuals' names, dates of birth, addresses, email addresses and bank account details. It can also include a randomly generated unique identifier or for example an IP address associated with IT equipment used by a sole user.*

The Information Commissioner's Officer provides further guidance on the meaning of personal data:

https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

Schedule 3 – Description of the Security Measures Under Clause 12

Signed by	....
for and on behalf of [NAME OF DATA DISCLOSER]	Position:
Signed by	....
for and on behalf of [NAME OF DATA RECEIVER]	Position:
Signed by	....
for and on behalf of [NAME OF DATA RECEIVER]	Position:
Signed by	....
for and on behalf of [NAME OF DATA RECEIVER]	Position: