

DATA SHARING AGREEMENT

between

[Insert [organisation name], a [organisation type – e.g. Local Authority/private company/charity] with registered number [registered number] and having its registered office/main office at [registered address]] (“XX”);

and

[Insert [organisation name], a [organisation type – e.g. Local Authority/private company/charity] with registered number [registered number] and having its registered office/main office at [registered address]] (“XY”),

each a “**Party**” and together the “**Parties**”.

Background

- (a) [INSERT BACKGROUND TO THE DATA SHARING, INCLUDING A BRIEF OUTLINE OF THE REASONS WHY THE DATA IS BEING SHARED]
- (b) The Parties are required to share Data between them for the Purpose as set out in the Schedule to this Agreement.
- (c) The Parties intend that this Agreement will form the basis of the data sharing arrangements between them. Nothing in this Agreement is intended to alter, supersede or in any other way affect the relationship between the Parties.
- (d) The intentions of the Parties are that they shall each be independent Data Controllers in respect of the Data that they Process under this Agreement.

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

- 1.1 In construing this Agreement (including the recitals), capitalised words and expressions shall have the meanings set out below:

“**Agreement**” means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;

“**Business Day**” means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;

“**Data**” means the information which contains Personal Data and/or Special Categories of Personal Data described in Part 1 of the Schedule;

“**Data Controller**” has the meaning set out in Data Protection Law;

“**Disclosing Party**” means the Party (being either XX or XY, as appropriate) disclosing Data (or on behalf of whom Data is disclosed to the Data Recipient);

“Data Protection Law” includes the Privacy and Electronic Communications (EC Directive) Regulations 2003; any legislation implementing the Privacy and Electronic Communications Directive 2002/58/EC of 12 July 2002; the General Data Protection Regulation (EU) 2016/679 of 27 April 2016 (GDPR); and any data protection legislation introduced in the United Kingdom, including the Data Protection Act 2018;

“Data Recipient” means the Party (being either XX or XY, as appropriate) to whom Data is disclosed;

“Data Subject” means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement are listed in Part 1 of the Schedule;

“Data Subject Request” means a request of either Party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the Data or the activities of the Parties contemplated by this Agreement;

“FOI Law” means the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004;

“Information Commissioner” means the UK Information Commissioner and any successor;

“Law” means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;

“Legal Basis” means in relation to either Party, the legal basis for sharing the Data as described in Clause 2.3 and as set out in Part 2 of the Schedule;

“Personal Data”, **“Special Categories of Personal Data”** and **“Processing”** each have the meanings ascribed to them in Data Protection Law and **“Process”** and any other tense or part of that verb will be interpreted accordingly;

“Purpose” means the purpose referred to in Part 2 of the Schedule;

“Representatives” means, as the context requires, the representative of XX and/or the representative of XY as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice by the relevant Party to the other Party;

“Request for information” means a request received by either Party in terms of FOI Law;

“Schedule” means the Schedule in 6 Parts annexed to this Agreement and a reference to a “Part” is to a Part of the Schedule; and

“Security Measures” has the meaning given to that term in Clause 2.4.5.

- 1.2 In this Agreement unless the context otherwise requires:
- 1.2.1 words and expressions defined in Data Protection Law shall have the same meanings in this Agreement;
 - 1.2.2 more generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions, consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder;
 - 1.2.3 words used in the singular will be interpreted to include the plural and vice versa and words which refer to one gender will be interpreted to include other genders;
 - 1.2.4 the words “**include**” and “**including**” shall each be construed without limitation to the words following; and
 - 1.2.5 where this Agreement defines a word or expression by reference to its meaning in Law and the Law changes such that the word or expression no longer has that (or any) meaning in Law then, for the purposes of this Agreement, the word or expression will be interpreted as referring to the term in Law then current which most nearly approximates to the meaning given to that word or expression before the Law changed.

2 DATA SHARING

Purpose and Legal Basis

- 2.1 The Parties agree to share the Data for the Purpose in accordance with the provisions of Part 2 of the Schedule.
- 2.2 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.
- 2.3 Each Party shall ensure that it Processes the Data fairly, lawfully and transparently consistent with Data Protection Law, including by providing Data Subjects with a privacy notice and each Party as Disclosing Party confirms to the other Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis in accordance with the provisions of Part 2 of the Schedule.

Parties Relationship

- 2.4 The Parties agree that the relationship between them is such that any Processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

- 2.4.1 it is a separate and independent Data Controller in respect of the Data that it Processes under this Agreement, and that the Parties are not joint Data Controllers or Data Controllers in common;
 - 2.4.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);
 - 2.4.3 it shall comply with its obligations under Part 6 of the Schedule;
 - 2.4.4 it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party; and
 - 2.4.5 it shall implement appropriate technical and organisational measures including, but without limitation, the security measures set out in Part 5 of the Schedule (the “**Security Measures**”), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its Processing of the Data, including, but without limitation, against unauthorised or unlawful Processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.
- 2.5 The Disclosing Party undertakes to notify the Data Recipient as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient to ensure that the Data Recipient is then able to correct its records.

Transferring Data

- 2.6 Subject to the Data Recipient’s compliance with the terms of this Agreement, the Disclosing Party undertakes to use reasonable endeavours to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

3 BREACH NOTIFICATION

- 3.1 Each Party shall, promptly (and, in any event, no later than 24 hours after becoming aware of the breach or suspected breach), notify the other Party of any breach or suspected breach of any of that Party’s obligations in terms of Clause 2 and of any other unauthorised or unlawful Processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):
- 3.1.1 the nature of the Personal Data breach or suspected breach;
 - 3.1.2 the date and time of occurrence;
 - 3.1.3 the extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by that party to contain the breach or suspected breach; and

- 3.1.4 any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.
- 3.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.
- 3.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in Law.

4 DURATION, REVIEW AND AMENDMENT

- 4.1 This Agreement shall come into force immediately on being executed by both Parties and continue for [INSERT TERM OF DATA SHARING], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.
- 4.2 This Agreement will be reviewed two years after it comes into force and every two years thereafter until termination in accordance with its terms.
- 4.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:
 - 4.3.1 the terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement;
 - 4.3.2 either Party reasonably believes that a change in Law necessitates an amendment to this Agreement; or
 - 4.3.3 the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.
- 4.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.
- 4.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:
 - 4.5.1 suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or

- 4.5.2 terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within ten (10) Business Days of receiving written notice of the breach.
- 4.6 Upon termination of this Agreement in accordance with Clause 4.1 or Clause 4.5, the Disclosing Party may request the return of the Data (in which case the Data Recipient shall, no later than twenty-eight (28) Business Days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part), save that the Data Recipient will be permitted to retain such copies for the purpose of complying with, and for so long as required by, any law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.
- 4.7 Upon termination of this Agreement (howsoever arising):
 - 4.7.1 the accrued rights, remedies, obligations and liabilities of the Parties as at termination shall not be affected, including the right to claim damages in respect of any breach of this Agreement which had occurred at or before the date of termination; and
 - 4.7.2 Clauses which expressly or by implication have effect after termination shall continue in full force and effect.

5 LIABILITY

- 5.1 Nothing in this Agreement limits or excludes the liability of either Party for:
 - 5.1.1 death or personal injury resulting from its negligence;
 - 5.1.2 any damage or liability incurred as a result of fraud by its personnel; or
 - 5.1.3 any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.
- 5.2 The Data Recipient indemnifies the Disclosing Party against any:
 - 5.2.1 losses, costs, damages, awards of compensation,
 - 5.2.2 any monetary penalty notices;
 - 5.2.3 administrative fines for breach of Data Protection Law; and/or
 - 5.2.4 expenses (including legal fees and expenses)

suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the Disclosing Party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms

of this Clause 5.2 is limited to £5,000,000 (FIVE MILLION POUNDS STERLING) in the aggregate for the duration of this Agreement.

5.3 Subject to Clauses 5.1 and 5.2 above:

5.3.1 each Party excludes all liability for breach of any conditions implied by Law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;

5.3.2 neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other Party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data under this Agreement; and

5.3.3 use of the Data by both Parties is entirely at their own risk and each Party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one Party from offering clarification and guidance to the other Party as to appropriate interpretation of the Data.

6 DISPUTE RESOLUTION

6.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

6.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.

6.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause 6.2, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

6.4 If mediation fails to resolve the dispute within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause 6.3 or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause 9.

- 6.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

7 FREEDOM OF INFORMATION

Where either Party receives a Request for Information in relation to any Data, or otherwise proposes to disclose such Data pursuant to its obligations under FOI Law, that party shall promptly notify the other Party and provide that other Party with a reasonable opportunity to make representations in relation to whether or not such Data is exempt from disclosure pursuant to FOI Law, provided that nothing in this Clause 7 shall fetter that Party's obligations to comply with FOI Law and shall not bind that Party to take into account or otherwise accept the representations of the other Party.

8 MISCELLANEOUS

8.1 No partnership or joint venture

This Agreement does not create a partnership or joint venture between the Parties to it, nor authorise either Party to act as agent for the other.

8.2 Waiver

No failure or delay by a Party in enforcing or exercising any right or remedy under this Agreement, or arising otherwise in Law in connection with this Agreement, will constitute a waiver of that right or remedy or an election to abandon that right or remedy in respect of any event or circumstances and, where applicable, to thereby affirm this Agreement, or will otherwise preclude or restrict the subsequent exercise of that or any other right or remedy. No single or partial exercise of such right or remedy will preclude or restrict the further exercise of that or any other right or remedy.

8.3 Notices

Any requirement to inform or notify a Party under or in connection with this Agreement shall be in writing, addressed to the relevant Party at the address noted in Part 4 of the Schedule or such other address as that Party may have specified to the other Party in writing in accordance with this Clause. It shall be delivered personally or sent by pre-paid first class post or other next working day delivery service, commercial courier or email. A notice or other communication shall be deemed to have been received:

8.3.1 If delivered personally, when left at the address referred to in Part 4 of the Schedule;

8.3.2 If sent by pre-paid first class post or other next working day delivery service, at 9.00am on the second Business Day after posting;

8.3.3 If delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed; or

8.3.4 If sent by email, one Business Day after transmission.

8.4 Unenforceable provision

If and to the extent that any provision of this Agreement is held to be invalid, unlawful or unenforceable by a court of competent jurisdiction, such provision will be treated as having been deleted from the remaining terms of this Agreement which will remain in full force and effect.

8.5 Entire agreement

This Agreement constitutes the entire agreement between the Parties in relation to its subject matter and supersedes any prior arrangement, understanding or agreement between them in relation thereto.

9 GOVERNING LAW

This Agreement and any dispute or claim arising out of or in connection with its subject matter or formation (including non-contractual disputes or claims) (a “**Dispute**”) shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

IN WITNESS WHEREOF these presents consisting of this and the preceding XXXX pages together with the Schedule in 6 parts hereto are executed by the Parties hereto as follows:

Executed for and on behalf of	XX	XY
Signature		
Name (Print)		
Job Title (Print)		
Date of Signature (Print)		
Location of Signature (Print)		
In the presence of this witness:		
Witness Signature		
Witness Name (Print)		
Witness Address (Print)		

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN XX AND XY

SCHEDULE PART 1: DATA

[INSERT DESCRIPTION OF DATA SETS TO BE SHARED AT CATEGORY LEVEL E.G. NAME, DATE OF BIRTH, JOB TITLE, ADDRESS, GENDER, ETC. IF THE PARTIES ARE TO SHARE DIFFERENT DATA SETS WITH EACH OTHER, THEN THIS MUST BE SPECIFIED]

DATA SUBJECTS

For the purposes of this Agreement, the Data of the following Data Subjects will be transferred between the Parties:

[INSERT DESCRIPTION OF DATA SUBJECTS BY CATEGORY E.G. EMPLOYEES, HOUSING APPLICANTS, ETC. IF THE DATA SUBJECTS DIFFER PER PARTY, THEN THIS MUST BE SPECIFIED].

Approved

SCHEDULE PART 2: PURPOSE AND LEGAL BASIS FOR PROCESSING DATA AND COMPLIANCE WITH DATA PROTECTION LAW

Purpose

XX and XY are sharing the Data in order to [INSERT DETAILED OUTLINE OF THE PURPOSE(S) UNDERLYING AND BENEFITS ASSOCIATED WITH THE DATA SHARING AND INCLUDE REFERENCES TO RELEVANT LEGISLATION (INCLUDING SPECIFIC PROVISIONS WITHIN LEGISLATION), WHERE APPROPRIATE.]

Legal Basis

Personal Data:

Under Data Protection Law, the Parties assert that the Legal Basis for the sharing of Personal Data further to this Agreement is that the Processing is necessary:

[INSERT RELEVANT LEGAL BASIS OR BASES]

Special Categories of Personal Data:

Under Data Protection Law, the Parties assert that the Legal Basis for the sharing of Special Categories of Personal Data further to this Agreement is that the Processing is necessary:

[INSERT RELEVANT LEGAL BASIS OR BASES]

Compliance with Data Protection Law

Under Data Protection Law, the Parties assert that they will comply with the principles contained in the Data Protection Law as follows:

[SET OUT HOW PARTIES WILL COMPLY WITH EACH GDPR DATA PROTECTION PRINCIPLE RELATIVE TO THIS DATA SHARING ARRANGEMENT. CROSS-REFERENCE MAY BE MADE TO E.G. PART 5 AND PART 6 OF THE SCHEDULE TO DEMONSTRATE COMPLIANCE WITH THE DATA SECURITY, DATA QUALITY AND DATA RETENTION PRINCIPLES, RESPECTIVELY.]

Data Protection Impact Assessment

The Parties have completed a Data Protection Impact Assessment (DPIA) of the data sharing set out in this Agreement. The outcome of the DPIA confirmed that privacy and the fundamental rights and freedoms of Data Subjects were being suitably addressed. The Parties agree that the DPIA must remain subject to review, particularly if the Purpose, the Data or Data Subjects are changed or if there are concerns as to whether the data sharing set out in this Agreement complies with the Data Protection Law.

[THE PARTIES MAY INSERT A COPY OF THE DPIA.]

SCHEDULE PART 3: DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of Data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent possible, the following media are used:

- [INSERT]

Approved

SCHEDULE PART 4: REPRESENTATIVES

Representatives and contact details

For XX:

Name:
Address:
Email:
Phone:

For XY:

Name:
Address:
Email:
Phone:

Escalation contact details:

For XX:

Name:
Address:
Email:
Phone:

For XY:

Name:
Address:
Email:
Phone:

Approved

SCHEDULE PART 5: SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

Any use of data Processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:

The unauthorised use of IT systems is prevented by:

- User ID
- Password assignment
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments
- Defined access levels

The following additional measures are taken to ensure the security of any Data:

- Network Username
- Network Password
- Application Username
- Application Password
- Application Permissions and access restricted to those who require it

3 Disposal of Assets

Where Data supplied by a Party no longer requires to be retained, any devices containing Data should be physically destroyed or the Data should be destroyed, deleted or overwritten using techniques to make the original Data non-retrievable and put beyond use, rather than using the standard delete or format function.

4 Malicious software and viruses

Each Party must ensure that:

4.1.1 PXX (or other equipment) used in supporting the service are supplied with anti-virus and security software of a standard commercially reasonable for these purposes and anti-virus and security updates are promptly applied. Such software shall be sufficient to ensure freedom of viruses, worms, Trojans or other hostile computer programs.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

5 Audit, Inspection and Testing

Each Party may audit the other Party's compliance with its obligations under this Agreement. This includes the right to inspect the relevant parts of the other Party's systems on which the Data is stored to ensure that appropriate Security Measures are in place, subject to such inspection taking place within a mutually agreed framework.

Approved

SCHEDULE PART 6: DATA GOVERNANCE

Data quality

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any Data, in excess of the Data noted in Part 1 of the Schedule, is shared, the Data Recipient will notify the Disclosing Party immediately and arrange the secure return of the Data and secure destruction of any copies of that Data.

Data retention and deletion rules

XX and XY shall independently determine what is appropriate in terms of their own requirements for data retention, in accordance with Data Protection Law and their internal data retention policies.

Data that is no longer required by a Party will be securely removed from its systems and any printed copies securely destroyed.

[XX AND XY MAY INSERT COPIES OF, OR LINKS TO, THEIR RESPECTIVE DATA RETENTION POLICIES, IF DESIRED.]

Data Subject Requests

The Parties shall respect and comply with Data Subject Requests in accordance with Data Protection Law and shall advise each other when a Data Subject Request is received by either of them from a Data Subject. The Parties shall keep records of Data Subject Requests received and their responses thereto, including any complaints made to, and investigations conducted by, the Information Commissioner.