Data sharing agreement

**THIS AGREEMENT IS DATED**

**Between**

1. X (registered charity number x) whose registered office is xxxx
and
2. Y (registered charity number y) whose registered office is at yyyy

Each **a Party** and together, **the Parties

Background**

1. The Parties are registered charities, regulated and registered by the Charity Commission.
2. Each Party provides grants for individuals and the Parties would like to work together to enable X to assess grant applications with Y for Z purpose.
3. In order to work together to deliver and administer grants, the Parties need to share personal information with each other about grant applicants on a regular and ongoing basis as specified in this Agreement.
4. In consideration of the benefits to the Parties of sharing the information subject to this Agreement, the Parties have granted the rights and accepted the obligations hereinafter appearing.

**Agreed Terms**

1. INTERPRETATION

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

* 1. Definitions:

|  |  |
| --- | --- |
| **Agreement:**  | this agreement, which is a free-standing document that does not incorporate any terms established by the Parties under separate contractual arrangements. |
| **Agreed Purpose:**  | has the meaning given to it in *clause 2* of this Agreement. |
| **Commencement Date:** | means the date of this Agreement. |
| **EEA** | means the European Economic Area which includes the countries or territories of the European Union in addition to Norway, Liechtenstein and Iceland. |
| **GrantsPlus** **ICO** | means the online portal administered by RLG through which grant applications are received. the regulator, the Information Commissioner’s Office, or any body carrying out the regulatory function under replacement EU or UK legislation. |
| **Deletion Procedure** **Direct Marketing**  | has the meaning given to it in *clause 8.1* to this Agreement.Has the meaning given to it in the DPA, namely, *the communication (by whatever means) of any advertising or marketing materials which is directed to particular individuals.* |
| **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 ICO’s Data Sharing Code of Practice of May 2011. |
| **Data Protection and Information Law** | the Data Protection Act 1998 (the DPA), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended) 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 ICO or any replacement EU or UK data protection or privacy legislation. |
| **Shared Personal Data**  | the Personal Data and Sensitive Personal Data to be shared between the Parties under clause 4 of this Agreement. |
| **Subject Access Request**  | (SAR) has the same meaning as "Right of access to personal data" in section 7 of the DPA. |
| **Working Day:**  | a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business. |

 **Data Controller**, **Data Processor**, **Data Subject**, **Personal Data**, **Sensitive Personal Data** **Processing** and **Appropriate Technical and Organisational Measures** shall have the meanings given to them in the DPA.

* 1. The Appendices 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 Appendices.
	2. Unless the context otherwise, requires, words in the singular shall include the plural and in the plural shall include the singular.
	3. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.
	4. A reference to a statue or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
	5. 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.
	6. A reference to **writing** or **written** includes email.
	7. Unless the context otherwise requires, the reference to one gender shall include a reference to the other genders.
1. PURPOSE

This Agreement sets out the framework for the sharing of **Personal Data** between the Parties as **Data Controllers**. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

* 1. The Parties consider this data sharing initiative necessary in order for them:
		1. to deliver and administer grant applications;
		2. to promote the interests of both Parties as registered charities;
		3. to monitor and evaluate the success of the grant awarding process and the success of the collaborative working between the Parties; and
		4. to manage and maintain records which need to be kept for the purposes of audit and inspection including by regulators, such as the Charity Commission.

The Parties shall not process the Shared Personal Data, as described in clauses 4.1 and 4.2 and Appendix 2, in a way that is incompatible with the purposes described in this clause 2.2 (the **Agreed Purpose**).

* 1. The Parties recognise the importance of processing the Shared Data in a secure and confidential manner which respects the privacy rights of the Data Subjects whose Personal Data is processed in accordance with this Agreement. This Agreement has therefore been drafted in accordance with **Data Protection and Information Law** and, in particular, in line with the ICO’s *Data Sharing Code of Practice (2011).*
		1. Each Party shall appoint a single point of contact (SPoC) who will work together to reach agreement with regard 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:
SPoC and Data Protection Officer (DPO) xxx
SPoC yyy

1. COMPLIANCE WITH DATA PROTECTION AND INFORMATION LAW
	1. Each Party must ensure compliance with the Data Protection and Information Law at all times during the Term of this Agreement.
	2. Each Party has a valid registration with the ICO which, by the time that the data sharing is expected to commence, covers the intended data sharing pursuant to this Agreement, unless an exemption applies.

The details are as follows:

* + 1. X ICO Registration number12345
		2. Y IC Registration number 678910
1. SHARED PERSONAL DATA
	1. The types of Personal Data that may be shared between the Parties during the Term of this Agreement are set out at Appendix 2.
	2. Subject to clause 5.3 below, the following types of Sensitive Personal Data may be shared between the Parties during the Term of this Agreement:
		1. Data Subject’s racial or ethnic origin;
		2. Data Subject’s religious or other beliefs of a similar nature;
		3. Data Subject’s physical or mental health or condition;
		4. Data Subject’s housing and employment status;
		5. Data Subject’s family situation – number and ages of family members
		6. Data Subject’s county of residence and which of the 4 UK nation’s they live in
	3. Further detail on the Shared Personal Data as described in clause 4.1 and clause 4.2 is set out in Appendices 2 to 4, together with any access and processing restrictions as agreed and established by the Parties.
	4. The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.
2. FAIR AND LAWFUL PROCESSING
	1. Each Party recognises that the sharing of the Shared Personal Data shall be on the basis of one or more of the following grounds under Schedule 2 of the DPA or any replacement EU or UK legislation:
		1. the Data Subject has provided his or her consent to the Processing of their Personal Data;
		2. processing is necessary for the performance of a task carried out in the public interest or in the exercise of any functions conferred on any person by or under any enactment; and
		3. processing is necessary for the purposes of the legitimate interests pursued by the Parties except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject.
	2. In addition to its obligations under clause 5.1, the items of the Shared Personal Data which fall into the category of Sensitive Personal Data shall only be shared on the basis of one ormore of the following grounds under Schedule 3 of the DPA or any replacement EU or UK legislation:
		1. the Data Subject has given his explicit consent, in writing to the processing of the Shared Personal Data for the purposes of grant assessment and distribution of grants, which may include cash awards or items.
		2. processing is for the purpose of the exercise of any functions conferred on any person by or under any enactment;
		3. processing relates to racial or ethnic origin and is necessary to review the existence or absence of equality of opportunity or treatment with a view to enabling such equality to be promoted or maintained;
		4. processing relates to religious belief or similar or physical or mental health or condition and is necessary to review the existence or absence of equality of opportunity or treatment with a view to enabling such equality to be promoted or maintained.
	3. The Parties to the Agreement shall, in respect of Shared Personal Data, ensure that their privacy notices are compliant with clear and provide sufficient information to the Data Subjects for them to understand what Personal Data is shared, the circumstances in which it will be share and the purposes for the data sharing.
	4. The Parties undertakes to inform the Data Subjects, in accordance with Data Protection and Information Law of the purposes for which it will process their Personal Data and provide all of the information that it must provide, to ensure that the Data Subjects understand how their Personal Data will be processed by the Parties and the identities or types of organisation with which the data will be securely shared.
	5. X’s Privacy Notice is set out at Appendix 4 and Y’s under Appendix 5.
3. DATA QUALITY
	1. The Parties agree to use compatible datasets and to record all Shared Personal Data using the methods as set out in Appendix 3.
	2. Shared Personal Data must be limited to the Personal Data described in clause 4.1 and clause 4.2, and Appendix 2of this Agreement.
4. DATA SUBJECTS' RIGHTS
	1. Data Subjects have a number of rights under Data Protection and Information Law, including the right to obtain certain information about the processing of their Personal Data through a Subject Access Request.
	2. Data Subjects may also request rectification, erasure or blocking of their Personal Data in circumstances where the processing of their Personal Data is not in compliance with Data Protection and Information Law.
	3. The Parties understand that where the Processing of any Personal Data is based upon a Data Subject’s consent or explicit consent under Data Protection and Information Law the Data Subject is entitled to withdraw their consent at any time for such processing by notifying the relevant Party in writing.
	4. Where the Processing of any Personal Data is based upon paragraphs 5 or 6 of Appendix 2 of the DPA or the equivalent provision under any EU or UK legislation (the ‘justice/enactments/crown/public functions ground’ or the ‘legitimate interests ground’), the Parties understand that Data Subjects have a right to object to the Processing of their Personal Data where the Processing is causing or likely to cause substantial unwarranted damage or distress to him or another individual (a ‘**Section 10 Objection’**).
	5. The Parties understand that where a Data Subject makes a Section 10 Objection, this must be made in writing and the Data Controller to whom the objection is addressed must respond within 21 calendar days of receipt of the notification in order to inform the Data Subject as to whether or not the organisation intends to comply with the notice or whether the objection is regarded as unreasonable and why.
	6. In instances where a Data Subject makes a Section 10 Objection in respect of any of the Shared Personal Data, the Party in receipt of the objection shall notify the other Party immediately or as soon as is practicably possible in order that both Parties may work together to address the complaint and deal with the objection fairly and expeditiously.
	7. SPoCs are responsible for maintaining a record of Subject Access Requests and Section 10 Objections, the decisions made and any information that was exchanged. Records must include copies of the Subject Access Request or Section 10 Objection, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request or complaint. The SPoCs for each Party are detailed in clause 2.3.1.
	8. The Parties agree to provide reasonable assistance as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other queries or complaints from Data Subjects.
5. DATA RETENTION AND DELETION
	1. The Parties shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes, and as required by any relevant sector guidance, including that issued by the Charity Commission, the Fundraising Regulator and the ICO and shall be processed in accordance with Parties’ data retention policies or schedules.
	2. The Parties shall ensure that any Shared Personal Data is destroyed in accordance with the agreed Deletion Procedure set out at Appendix 3 in the following circumstances:

		1. on termination of the Agreement;
		2. once processing of the Shared Personal Data is no longer necessary for the purposes for which they were originally shared, as set out in clause 2.4.
	3. Following the deletion of Shared Personal Data in accordance with clause 8.2, the each Party shall inform the other that the Shared Personal Data in question has been deleted in accordance with the Deletion Procedure at Appendix 3 to this Agreement.
6. INTERNATIONAL DATA TRANSFERS AND CLOUD COMPUTING
	1. For the purposes of this clause, international transfers of Personal Data (‘**International Data Transfers’**) shall mean any disclosure of the Shared Personal Data by either Party outside of the EEA and includes, but is not limited to, the following circumstances:
		1. storing Shared Personal Data on computer servers or within a data centre located outside of the EEA, which may occur where a cloud storage solution is used.
		2. Sub-contracting the processing of Shared Personal Data to Data Processors located outside of the EEA.
		3. granting third parties located outside of the EEA access rights to the Shared Personal Data.
	2. Neither Party shall make an International Data Transfer to a Data Controller entity.
	3. Either Party may make an International Data Transfer where the third party to whom the Shared Personal Data is disclosed is:
		1. a Data Processor and;
		2. the transfer of the Shared Personal Data is made in accordance with Data Protection and Information Law, and in particular, in accordance with Principles 7 and 8 of the DPA or any replacement EU or UK legislation.
	4. Subject to clause 9.3 above, where either Party wishes to use a cloud solution in respect of any of the Shared Personal Data the Parties agree that the guidance issued by the ICO or any replacement regulator shall be followed.
7. SECURITY AND TRAINING
	1. The Parties shall only provide the Shared Personal Data to each other by using the secure method as agreed and set out in Appendix 2.
	2. Having regard to the state of technological development and the cost of implementing such measures, the Parties have in place Appropriate Technical and Organisational Measures as set out in Appendix 5 in order to:
		1. prevent:
			1. unauthorised or unlawful processing of the Shared Personal Data; and
			2. the accidental loss or destruction of, or damage to, the Shared Personal Data
		2. ensure a level of security appropriate to:
			1. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
			2. the nature of the Shared Personal Data to be protected.
	3. It is the responsibility of each Party to ensure that its staff members and any third party data controllers such as consultants and advisers which it appoints are appropriately trained to handle and process the Shared Personal Data in accordance with the Appropriate Technical and Organisational Measures relating to security set out in Appendix 4.
	4. The Parties agree that where they appoint third party Data Controllers such as consultants or advisers they will conduct the requisite degree of due diligence in advance of any such appointment to ensure that such third parties are aware of their responsibilities under Data Protection and Information Law when handling the Shared Personal Data.
	5. Where either Party appoints a third party individual or organisation to process the Shared Personal Data on its behalf as a Data Processor it shall ensure that any such individual or organisation is appointed in accordance with Principle 7 of the Data Protection Act 1998 or any replacement EU or UK legislation which requires that:
		1. the processing is carried out under a contract in writing and;
		2. under which the Data Processor is to act only on instructions from the relevant Party as data controller, and;
		3. the data processing contract requires the Data Processor to comply with obligations equivalent to those imposed on a data controller by the seventh data protection principle.
	6. The Parties agrees to allow each other to process the Shared Personal Data for the Agreed Purpose only on the clear understanding that each Party does not share any Personal Data supplied to it with any person within or outside of the Parties otherwise than;

		1. in accordance with this Agreement and on a need-to-know basis only;
		2. in accordance with a legal obligation, including court order; or
		3. with the prior written, explicit consent of the grant applicant.
8. COMPLAINTS, DATA SECURITY BREACHES AND REPORTING PROCEDURES
	1. Having considered Data Protection and Information Law, the Parties have in place their own guidance that must be followed in the event of a Data Security Breach.
	2. Parties are under a strict obligation to notify any potential or actual losses of the Shared Personal Data or any breach of security which may compromise the security of the Shared Personal Data to each SPoC as soon as possible and, in any event, within 2 working day(s) of identification of any potential or actual loss to enable the Parties to consider what action is required in order to resolve the issue in accordance with Data Protection and Information Law.
	3. The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Data Security breach in an expeditious and compliant manner, which shall include, but may not be limited to, immediate co-operation between each SPoC in order to determine the required action any possible notification to the ICO or affected Data Subjects where deemed necessary.
	4. In the event of a Data Security Breach this Agreement can be suspended for 10 working days by either Party whilst investigations take place by a panel represented by signatories to this Agreement.
9. REVIEW AND TERMINATION OF AGREEMENT
	1. This Agreement shall commence on the Commencement Date and shall be reviewed on a six monthly basis by the SPoC having consideration to the aims and purposes set out in clause 2.4. The Parties shall continue, amend or terminate the Agreement depending on the outcome of this review.
	2. The review of the effectiveness of the data sharing initiative will involve:
		1. assessing whether the purposes for which the Shared Personal Data is being processed are still the ones listed in clause 2.4 of this Agreement;
		2. assessing whether the Shared Personal Data is still as listed in clauses 4.1 and 4.2 of this Agreement;
		3. assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and
		4. assessing whether personal data breaches involving the Shared Personal Data have been handled in accordance with this Agreement and the applicable legal framework.
	3. Both Parties reserve the right to inspect each Parties arrangements for the processing of Shared Personal Data and to terminate the Agreement where it considers that the other Party is not processing the Shared Personal Data in accordance with this Agreement.
10. PARTIES’ OBLIGATIONS

Each Party agrees that it shall:

* + 1. process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its Personal Data processing operations;
		2. respond within 2 working days and as far as reasonably possible to enquiries from the ICO in relation to the Shared Personal Data;
		3. respond to Subject Access Requests and Section 10 Objections in accordance with Data Protection and Information Law;
		4. maintain its registration with the ICO to process all Shared Personal Data for the Agreed Purpose;
	1. take all appropriate steps to ensure compliance with the security measures set out in clause 10 above.
1. DIRECT MARKETING
	1. If either Party receives and Processes the Shared Personal Data for the purposes of Direct Marketing, each Party shall ensure that:
		1. The appropriate explicit consent has been obtained from the relevant Data Subjects to allow the Shared Personal Data to be used for the purposes of Direct Marketing in compliance with Data Protection and Information Law; and
		2. Effective procedures are in place to allow the Data Subject to opt-out from having their Shared Personal Data used for Direct Marketing purposes.
2. liability
	1. Each Party shall accept responsibility for its own acts and omissions and will be solely responsible for any and all costs, expenses, claims and liabilities arising out of any breach of this Agreement on its part.
	2. Neither Party excludes nor limits liability to the other Party for death or personal injury caused by its negligence or fraud.
	3. Each Party agrees to indemnify and keep indemnified and defend at its own expense the other Party against all costs, claims, damages or expenses incurred by the other Party or for which the other Party may become liable due to any failure by the first Party or its employees or agents to comply with any of its obligations under this Agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure of data obtained in connection with this Agreement by its subcontractors, employees, agents or any other person within its control.

**Appendix 1 - Key legislative provisions and authoritative guidance**

This Appendix sets out some of the key guidance and legislation but is not an exhaustive list

*The Data Protection Act 1998;*

*The Human Rights Act 1998;*

*The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) (as amended);*

*The Safeguarding Vulnerable Groups Act 2006 as amended;*

*The Equality Act 2010;*

*Protection of Freedoms Act 2012.*The common law duty of confidentiality will also apply to the Processing carried out by each Party to this Agreement

Guidance and Codes of Practice issued by the ICO, including:

*The Data Sharing Code of Practice (2011);*

*Direct Marketing guidance (2016);*

*Guidance on Privacy and Electronic Communications Regulations (2016);*

*Subject Access Code of Practice 2014;*

*Guidance on data security breach management 2012;*

*Notification of data security breaches to the Information Commissioner’s Office 2012;*

*Encryption 2016;*

*Guidance on the use of cloud computing (2012);*

*Deleting Personal Data 2014.*

Guidance issued by the Fundraising Regulator

*Personal Information & Fundraising: Consent, Purpose and Transparency (2017)*

Appendix 2 – Agreed mechanism for transfer of the Shared Personal Data

When sharing personal data between X and Y:

X will use (please specify here)

Y will use (please specify here).

Appendix 3 - Appropriate Technical and Organisational Security Measures

Each Party shall adhere to its own Information Security and data breach reporting policies and procedures and shall ensure as a minimum that:

* The level of security to be applied to any particular items of Personal Data should depend upon the sensitivity of that data – items of Sensitive Personal Data will require a higher level of security;
* the transfer of the Shared Personal Data shall be carried out only in accordance with the secure methods set out at Appendix 2;
* unauthorised staff and other individuals are prevented from gaining access to the Shared Personal Data and that access to confidential parts of the each Party’s management information system is on a role-appropriate password-controlled basis;
* Written clauses in employment contracts should ensure that staff maintain confidentiality and operate in accordance with each Party’s policies and procedures;
* Human Resources procedures are in place to ensure the reliability of staff and to provide for disciplinary procedures for non-compliance issues;
* All electronic, including portable electronic devices which are used for processing the Shared Personal Data are protected with appropriate anti-malware software and are encrypted;
* Where any electronic device is used to store any of the Shared Personal Data the data is securely removed before disposal;
* All paper files containing the Shared Personal Data are securely stored in lockable cabinets, accessible on a role-appropriate basis, and securely destroyed when no longer needed, according to each Parties retention, archiving and deletion policy;
* All staff are regularly trained in data protection, including data security and are aware of the requirement not to leave workstations or computers signed on when accessing the Shared Personal Data; the requirement for use of strong passwords and that these should not be shared; to lock away memory sticks and printouts containing the Shared Personal Data when not in use;
* Shared Personal Data should only be sent by email if the transmission is encrypted;
* Shared Personal Data should only be sent by fax in exceptional circumstances and, then only where the intended recipient is aware of the transmission and can ensure security on receipt.
* (please specify deletion procedures here …)

Appendix 4 – X Privacy Statement

Please insert below.

Appendix 5 – yyyy Privacy Statement

(please insert below)

Signed by:

For and on behalf of X
Date:

Signed by:

For and on behalf of Y
Date: