1 Introduction

1.1 In its everyday operations Foundation Scotland [FS] makes use of a variety of data about identifiable individuals, including data about:

- Clients
- Current, past and prospective employees
- Donors
- Grant Recipients
- Community Panel members
- Users of its website
- Other stakeholders

1.2 In collecting and using this data, FS is subject to legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it. The purpose of this policy is to set out the relevant legislation and to describe the steps FS is taking to ensure compliance with it.

2 Scope

2.1 This policy applies to all systems, people and processes that constitute FS's information systems, including board members, committee members, employees, suppliers and other third parties who have access to FS's systems.

3 Abbreviations and Definitions

Abbreviations

- CFOO – Chief Finance and Operations Officer
- DPO – Data Protection Officer
- GDPR - General Data Protection Regulation
- ICO – Information Commissioner's Office
- LMS – FS's Learning Management System

Definitions

3.1 There are 26 definitions listed within the GDPR. The most important definitions with respect to this policy are:

- Data Subject - identified or identifiable natural person[s].
- Personal data - any information relating to an identified or identifiable natural person [Data Subject]; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, 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.
- Controller - the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

4 Policy

GDPR

4.1 The GDPR is one of the most significant pieces of legislation affecting the way that FS carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of individuals. It is FS's policy to ensure that our compliance with the GDPR and other relevant legislation is always clear and demonstrable.

Principles Relating to Processing of Personal Data

4.2 There are six fundamental principles upon which the GDPR is based. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject [lawfulness, fairness, and transparency]
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be incompatible with the initial purposes [purpose limitation]
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed [data minimisation]
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay [accuracy]
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject [storage limitation]
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures [integrity and confidentiality]

4.3 The controller is responsible for and be able to demonstrate compliance with the above.

4.4 FS ensures that it complies with all these principles, in the processing it currently carries out and as part of the introduction of any new methods of processing such as new IT systems.

Rights of the Individual

4.5 The data subject also has rights under the GDPR.

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

4.6 Each of these rights are supported by appropriate procedures within FS that allow the required action to be taken within the timescales stated in the GDPR. These timescales are shown in the table below.

Data Subject Request	Timescale
The right to be informed	When data is collected [if supplied by data subject] or within one month [if not supplied by data subject]
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not specified [However FS does not currently operate automated decision making]

Lawfulness of Processing

4.7 There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is FS policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

- Consent Unless it is necessary for a reason allowable in the GDPR, FS will always obtain explicit consent from a data subject to collect and process their data. In case of children below the age of 16 consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge. If the personal data are not obtained directly from the data subject then this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within one month.

- Performance of a Contract Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a grant payment cannot be made without an address to send it to.
- Legal Obligation If the personal data is required to be collected and processed to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example.
- Vital Interests of the Data Subject In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. FS will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. FS does not currently process data in this category.
- Task Carried Out in the Public Interest Where FS needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required. FS does not currently process data in this category.
- Legitimate Interests If the processing of specific personal data is in the legitimate interests of FS and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

Sensitive Personal Data

4.8 FS understands the additional protection which requires to be afforded to special category data [sensitive data] as this type of data creates the most significant risks to a person's fundamental rights and freedoms – for example by putting them at risk of unlawful discrimination. Examples of sensitive data include information about an individual's health or ethnic origin.

4.9 FS will generally not collect and use such data unless processing is required to demonstrate fulfilment of criteria for the award of funding and the data subject has supplied this information themselves or we need it to fulfil our obligations as an employer. Likewise, FS will only carry out criminal record checks in certain limited circumstances.

Privacy by Design

4.10 FS has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments. The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose[s].
- Assessment of the risks to individuals in processing the personal data.
- What controls are necessary to address the identified risks and demonstrate compliance with legislation.

4.11 Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

Sharing of Personal Data

4.12 FS may from time to time, share personal data we hold with third parties. This will occur when it is required to carry out its business functions and charitable activities or where there is a legal obligation to do so.

Contracts Involving the Processing of Personal Data

4.13 FS will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR. For more information, see the GDPR Controller-Processor Agreement Policy

International Transfers of Personal Data

4.14 Transfers of personal data outside the UK will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR.

Data Protection Officer

4.15 A defined role of DPO is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider. Based on these criteria, FS does not require a Data Protection Officer to be appointed. However, the CFOO will provide advice and support on such matters as required.

Breach Notification

4.16 It is FS's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. All GDPR incidents are recorded in RiskMate. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the ICO will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

4.17 Under the GDPR the ICO has the authority to impose a range of fines of up to four percent of annual worldwide turnover or £17.5m, whichever is the higher, for infringements of the regulations.

Addressing Compliance to the GDPR

4.18 The following actions are undertaken to ensure that FS always complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous.
- The CFOO has specific responsibility for data protection in FS.
- All staff involved in handling personal data understand their responsibilities for following good data protection practice.
- Training in data protection has been provided to all staff.
- Rules regarding consent are followed.

- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
- Regular reviews of procedures involving personal data are carried out.
- Privacy by design is adopted for all new or changed systems and processes.

4.19 The following documentation of processing activities is recorded:

- Organisation name and relevant details.
- Purposes of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
- Personal data retention schedules
- Relevant technical and organisational controls in place

4.20 These actions are reviewed on a regular basis as part of the management process concerned with data protection.

5 Roles and Responsibilities

5.1 All those mentioned in 2.1 have a responsibility to ensure compliance with the GDPR and this policy, and to develop and encourage good information handling practices.

6 Training

6.1 The following courses are mandatory for FS staff [* and for Trustees and Co-opted Committee Members]

- LMS – Data Protection *
- LMS – General Data Protection Regulation *
- T001 – General Data Protection Regulation 1 – Keeping Our Information Secure
- T002 – General Data Protection Regulation 2 – An Introduction

7 References

- Information Commissioner's Office https://ico.org.uk
- FS Privacy Notice https://www.foundationscotland.org.uk/privacy-policy

8 Review

8.1 This policy is reviewed, approved, and endorsed by the Board of trustees. It is updated when required by legislation, to ensure that it reflects statutory responsibilities, government guidance and best practice for FS or every 24 months whichever is the soonest.