DATA PROTECTION POLICY

1. Purpose and Scope

Esmée Fairbairn Foundation ("the Foundation") needs to keep certain information about its employees, partners and organisations which apply to it for funding, including those which are unsuccessful. This allows it to monitor performance, keep track of financial dealings and be compliant with statutory duties, for example.

To comply with the law, information must be collected and used fairly, stored safely and not beyond a reasonable point and not disclosed unlawfully. The Foundation therefore complies with the Data Protection Principles set out in the Data Protection Act 1998 ("DPA") and the General Data Protection Regulation ("GDPR").

The DPA principles state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Anyone who processed data on behalf of the Foundation must ensure that they follow these principles always. In order to ensure that this happens, the Foundation has developed the Data Protection Policy.

2. Definitions

The policy covers all employees. Others who work with the Foundation such as temporary agency staff, trustees and consultants, will also be required to follow the legislation.

The term "**data processing**" is very widely defined in DPA and includes obtaining, recording, organising, using, disclosing, deleting, and simply holding data (information). Therefore, anything you do with information will amount to processing.

The term "**personal data**" is data that relates to a living individual who can be identified from that data or from any other information that is in (or is likely to come into) the possession of the data controller (person processing the data).

There is a sub-category of personal data which is referred to in the DPA as "**sensitive personal data**" and there are even more obligations on those who process this data. Sensitive personal data is information that relates to an individual's political opinions, racial or ethnic origins, mental or physical health, sexual life, religious persuasion, trade union affiliation or criminal record.

The DPA covers data held in non-electronic form, such as paper files as well as any held on computer or other electronic storage.

3. Responsibilities

a. Roles

Role	Staff Role	Responsibility
Senior Information Risk Owner (SIRO)	Chief Operating Officer	Manage response to breaches of the policy. Communicate major breaches to the Chair of the ARC. Work with the Technology Lead to put preventative measures and resolutions in place.
Salesforce Lead	Salesforce System Administrator (Technology Lead, supported by Operations Lead)	Oversight of Salesforce (CRM), to raise issues about data storage and security to the SIRO and to ensure the retention schedule is adhered to.
Trustee Leads	Audit and Risk Committee	Oversight of the organisation policy, to be informed of any breaches and work with the SIRO and Technology Lead to agree measures to be taken in the event of a breach.

b. Information about staff

In regard to information about themselves, staff are responsible for:

- Checking that any information that they provide to the Foundation in connection with their employment is accurate and up to date.
- Informing the Foundation of any changes to information, which they have provided, e.g. changes of home address.
- Informing the Foundation of any errors or changes in staff information. The Foundation cannot be held responsible for any such errors unless the staff member has informed them.

c. Information about others

All staff are required to maintain confidentiality in their work as appropriate. However, in relation to personal data it is essential to review procedures for handling this data to ensure that all processing is lawful under DPA.

- Access to personal data should be restricted to those who need it for clearly defined purposes. Personal data held on computer should be protected by regularly changed passwords, whilst data held in other ways should be kept secure when not in use. Special care should be taken when data is being moved around externally, e.g. when carrying laptops, and data should be encrypted. Failure to protect against unauthorised access would be an offence under DPA.

- Data must only be used for purposes for which it is collected. Data collected for one purpose must not be used for other purposes unless these were made known at the time the data was collected, or the data subject is advised and consents.

- Data should not be held for longer than necessary and so should be destroyed when no longer needed, or at the end of any statutory retention period. Only keep data if there is a good reason for doing so – getting rid of unnecessary data can also save on space. Data should be destroyed appropriately, which will usually involve shredding. Care must be taken not to throw personal data into general waste bins.
- Take care when revealing third party personal data to anyone other than the individuals themselves. Where necessary, obtain appropriate evidence of identity and establish why the data is needed. Consider whether or not revealing the data is in accordance with the DPA, and if in doubt, seek advice from the SIRO. The consent of the data subject should be obtained whenever possible.
- It is advisable for everyone working at or with the Foundation to review their data processing on a regular basis, to ensure compliance with the legal principles. Individuals should consider how long to retain the personal data that is relevant to their area of work and put together appropriate guidelines for destroying data, together with systems to ensure that these guidelines are followed.
- Data should not be shared with third parties – including SaaS (software as a service) tools – without consideration of both GDPR and the DPA. This includes uploading data to "AI" tools such as ChatGPT without prior approval from the relevant staff roles.

d. Right to Access Information

Staff, grantees and other partners of the Foundation have the right to access any personal data that is being kept about them either on a computer or in hardcopy files.

Any person who wishes to exercise this right should contact the SIRO, in writing. Data should not be given out by staff over the phone, due to the difficulty in verifying identities.

Data can be disclosed to a third party without the consent of the data subject in the following circumstances only:

- Data required by law e.g. data supplied to statutory bodies.
- Data that is in the vital interests of the data subject.
- Data that would prevent harm to a third party.
- Data that would prevent crime.
- Data that would be in the interest of national security.

A record must be kept on file of any disclosure, including date, to whom, and the reason for the request.

The Foundation aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days.

Exemptions to access

Access may not be permitted in the following circumstances:

- The data subject has not provided sufficient information to enable the SIRO to satisfactorily identify the data subject or otherwise comply with the request.
- The Foundation has already complied with the same or a similar request within a reasonable period.
- Disclosure of the data would also disclose information relating to another individual unless:
    - the other individual has consented; or
    - it is reasonable to disclose the information without such consent.

Careful consideration should be given to what is "reasonable", in relation to the last point, thinking through any duty of confidentiality owed to the other individual, any steps that the data controller might take to seek consent from them, and whether the other individual is capable of consenting, e.g. they may have left the organisation without a forwarding address.

4. Relevance

The Foundation holds personal data on its employees, some of which is sensitive and some of which is shared with Moorepay (the Foundation's payroll processing partner). Within the organisation this information is only accessible to the Chief Operating Officer (who acts as the SIRO) and in their absence the CEO, Head of Finance and Finance Officer.

Whilst not in a personal context; as the information is provided to Esmée in the context of an organisation which is requesting funding. The Foundation holds contact details of people who have applied for grants or social investments, some of this information, such as the email address may be for personal and professional use. This has been volunteered to the organisation and contact details have been supplied in the context of the person being employed or otherwise acting on behalf of an organisation.

The Foundation holds contact details of some interested parties, such as those who have asked to be sent copies of Annual Reports, those who work in partnership with the organisation or those who work with our finance team.

The Foundation holds a significant amount of data which does not classify as personal under DPA or GDPR, such as organisational details and information about investments it has made. Whilst not subject to the same level of rigor under DPA we have ensured there is a retention period attached to this data.

5. Processing

The Foundation holds employee information and acts as a joint controller with MoorePay with regard to payroll. This is held for the legal and justifiable reasons, with employees being able to access the information that is held about them. Other information related to HR, such as interview notes for unsuccessful applicants is held for the appropriate amount of time and then destroyed.

The Foundation deals in little which would be classed as direct marketing. It sends emails and information to potential and current grantees, however these are expected as part of the grant process and do not feature marketing about the Foundation or its activities. Most activity which could be classed as marketing is done via twitter or our website where people can choose to engage. The Foundation electronically sends its Annual Report to current grantees, key partners and other parties that have asked to be sent it.

There are some instances where staff members may wish to use "AI" tools, such as Zoom transcription services, or ChatGPT, in order to more efficiently handle the processing of data. Where this is being done, extreme caution should be taken to ensure that no sensitive data is being collected, or processed, without the explicit permission of the Data subject. At all times, the ICT Policy should be adhered to when using these tools.

6. Data Retention

Data Retention Schedule.

Data	Retention	Comment

Ex-employee information	10 years after leaving (other than basic details of name, role and dates retained)	
Applicants for jobs, consultancy tenders or similar who are not shortlisted for interview	6 months after the closing date	
Applicants shortlisted for job, consultancy or similar interview who are not successful	6 months after the interview date	
Details about grants and social investment to organisations	Ongoing – information kept as may inform future decisions and so there is a complete record of charitable funding.	
Details about grants and social investment that were unsuccessful	Ongoing – basic information kept so a full record of past applications	
Investment information, Social Investment financial information, Financial information	7 years after the end of the investment/contract/financial year.	

7. Disposal of Data

7.1 Disposal of physical data

Physical (manual) records that require destruction are securely saved and then a commercial shredding company is used to destroy them. There is an office shredder available for immediate shredding of smaller documents.

7.2 Disposal of hardware

When hardware containing data (e.g. company laptops, servers, etc) reaches the end of its serviceable life, it must be securely destroyed, or securely wiped ready for redistribution (in the case of laptops that are going to be recycled). When this happens, the Foundation's IT Supplier is contacted to either perform the work themselves, or provide recommendations on reputable suppliers for this work.

Certificates of destruction / erasure must be obtained for each device. If destruction/erasure is happening off-site, then a chain of custody certificate (or equivalent certification) must be obtained before the hardware is released.

Approved by Audit and Risk Committee 10.06.2025