THE FRANK SOO FOUNDATION

Data Protection Policy

Content

Introduction and Scope
Date Protection Lead
Data Protection
Date Protection Principles
Individual Rights
Use of Imagery/Video
Date Breach
Other Policies
Fund Raising
AI
Data Retention

Introduction and Scope

This policy outlines The Frank Soo Foundation's commitment to data protection and compliance with the UK Data Protection Act. The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of The Frank Soo Foundation, including trustees, staff, and volunteers.

Data Protection Lead

The Frank Soo Foundation will appoint a Data Protection Lead who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities.

Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is a UK law that regulates the processing of personal data. The UK Information Commissioner's Office (ICO) provides guidelines on data protection that The Frank Soo Foundation will follow.

UK GDPR: The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
Data Processor: An individual or organisation that processes personal data on behalf of a data controller.
Data Controller: An individual or organisation that determines how and why personal data is processed.
Data Subject: An individual whose personal data is being processed.
Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.
Personal Data: Any information that can identify a living individual, such as name, address, or email address.
Sensitive Personal Data: Personal data that requires extra protection, such as health information or ethnic origin.
Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.
PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.
Valid Consent: Consent given freely, specifically, and informed, and can be withdrawn at any time.
Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Data protection principles

Data is:

- **Processed lawfully, fairly and in a transparent manner.**
    - There are several grounds on which data may be collected, including consent.
    - We are clear that our collection of data is legitimate and we have obtained consent to hold an individual's data, where appropriate.
    - We are open and honest about how and why we collect data and individuals have a right to access their data.
- **Collected for specified, explicit and legitimate purposes and not used for any other purpose.**
    - We are clear on what data we will collect and the purpose for which it will be used.
    - And only collect data that we need.
    - When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.
- **Adequate, relevant and limited to what is necessary.**
    - We collect all the data we need to get the job done.
    - And none that we don't need.
- **Accurate and, where necessary, kept up to date.**
    - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.
    - We correct any mistakes promptly.
- **Kept for no longer than is necessary**. We understand what data we need to retain, for how long and why.
    - We only hold data only for as long as we need to.
    - That includes both hard copy and electronic data.

- Some data must be kept for specific periods of time (eg accounting, H&SW).
- We have some form of archive/review policy/process that ensures data no longer needed is destroyed.

- **Processed to ensure** appropriate security, not only to protect against unlawful use, but also loss or damage.
  - **Data is held securely**, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected.
  - **Data is kept safe.** Our IT systems have adequate anti-virus and firewall protection that's up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
  - **Data is recoverable.** We have adequate data back-up and disaster recovery processes.

Individual Rights

What are your data protection rights?

a) We would like to make sure you are fully aware of all your data protection rights. Every user is entitled to the following:

i. The right to access – you have the right to request copies of your personal data from us.

ii. The right to rectification – you have the right to request that we correct any information you believe is inaccurate. You also have the right to request that we complete any information you believe is incorrect.

iii. The right to erasure – you have the right to request that we erase your personal data, under certain conditions.

iv. The right to restrict processing – you have the right to object to our processing of your personal data, under certain conditions.

v. The right to object to processing – you have the right to object to us processing your personal data, under certain conditions.

vi. The right to data portability – you have the right to request that we transfer the data that you have given us to another organisation, or directly to you.

vii. You have rights in relation to automated decision making and profiling. The Frank Soo Foundation does not use any of your personal data to make automated decisions however we do create a profile of you and you can request that we stop doing this.

b) If you would like to exercise any of the above rights, please contact us at:

i. Email us at - info@thefranksoofoundation.org.uk

ii. Or write to us at –

The Frank Soo Foundation
Mulberry Grn,
Old Harlow,
Harlow
CM17 0ET

We will deal with your request within one calendar month of receiving it.

Use of Imagery/Video

All imagery is protected by copyright and cannot be used without the consent of the owner, usually the person who took the image. You may also need consent from the individuals in images of individuals and small groups, which may well fall within the Data Protection Act. However, there is some ambiguity, so err on the side of caution and obtain consent wherever this is reasonably possible. Particular care is to be taken when using images of children or other vulnerable people.

Here are some questions to consider when using imagery:

- For what purpose was the original image taken? If it was for one purpose, such as personal use, it cannot be used for another without the consent of the individuals concerned
- Is the image sensitive personal data? If it is, do you have the individual's consent?
- For small groups and individuals, has an image consent form been used?
- When using images of children, or people who may not be competent, do you have valid consent?

- When using images of children or other vulnerable people, are you confident your use of the image will not place them at risk? Particularly, if it is to be used publicly, such as in the Media or on the web.
- When photographing large groups, have the individuals been given a chance to opt out of the photograph?
- Has the person/people in the image been told how the image will be used?
- Are you using the image according to how the person/people were told it would be used?

Data Breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where there will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence.

The data protection lead will be notified within 48 hours who will notify the ICO within 72 hours, of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- Result in discrimination.
- Damage to reputation.
- Financial loss.
- Loss of confidentiality or any other significant economic or social disadvantage.

Other Policies

Children

People under 18 years of age are not legally able to give consent. You may also wish to ensure that privacy notices, or other information you give them, are written and presented in a way that is understandable and fair.

People Who Are Not Competent

Some people are unable, or may be unable to give consent, and this must be obtained from the person who is able to make decisions on their behalf, such as a Lasting Power of Attorney. Any decisions that you may make on their behalf, must always be in their best interests.

Vulnerable Groups

Special Category Data

Special category (sensitive) data is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

All special category data will be stored with extra care; using password protected access or have restricted views on our Google Suite.

International Data Transfers

There are specific rules when transferring data to another country. Here is the guidance relating to Brexit.

Privacy And Electronic Communications

Known as PECR, there are special regulations covering electronic marketing messages (by phone, fax, email or text), cookies and electronic communication services to the public.

Fundraising

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors.

Fundraising Preference Service

We will respect the privacy and contact preferences of our donors. We will respond promptly to requests to cease contacts or complaints and act to address their causes.

Artificial Intelligence

We have adopted and comply with the Charity AI Ethics & Governance Framework and ICO AI guidance.

Data Retention

Our data will only be kept for as long as there is an administrative need to do so in order to enable our charity to carry out its business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or to meet legislative requirements.

In general, records are kept for 6 years after the end of the accounting year to which they relate but we do not keep personal records any longer than necessary and certain records may be required to be retained for longer. Factors affecting retention periods include legal requirements, storage costs, historical value, industry standards, and archival needs.

Version Control - Approval and Review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	27/08/25	Initial draft approved	Annually