DATA PROTECTION POLICY

Introduction

France Mission needs to gather and use certain information about individuals.

These can include supporters, donors, mission partners, employees, volunteers and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Mission's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures France Mission:

- Complies with data protection law and follow good practice
- Protects the rights of staff, supporters, donors and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 (DPA) describes how organisations — including France Mission must collect, handle and store personal information.

The DPA incorporates the EU General Data Protection Regulations (GDPR) which strengthens the rights of individuals to know what personal information is held by an organisation, how long it will be retained for and how they can request that it is amended or deleted. It also requires organisations to evidence that they have the consent of the individual to their personal data being collected, processed and retained.

These regulations apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The DPA is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects

7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The Trustees of France Mission
- All staff and volunteers of France Mission
- All contractors, suppliers and other people working on behalf of France Mission

It applies to all data that the Mission holds relating to identifiable individuals, even if that information technically falls outside of the DPA. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Social media identities
- Bank details of donors
- Register of gifts made and the donor
- Relevant notes concerning previous involvement with the Mission or mission related work in France
- Detailed personal and contractual information relating to employees only

Data protection risks

This policy helps to protect France Mission from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the Mission uses data relating to them.
- **Reputational damage.** For instance, the Mission could suffer considerable damage if unauthorised persons successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with France Mission has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The Trustees are the Data Controller and therefore are ultimately responsible for ensuring that France Mission meets its legal obligations.

The **UK Director, Paul Cooke,** is responsible for:

- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Assisting in the evaluation of any third-party services the Mission is considering using to store or process data. For instance, cloud computing services, customer relations management systems or publicity organisations.
- Where necessary, working with other staff and volunteers to ensure communication and other initiatives abide by data protection principles.

The **Trustee responsible for Data Protection, Adrian Walter,** is responsible for:

- Ensuring all Mission systems, services and equipment used for storing data meet acceptable security standards.
- Evaluating any third-party services the Mission is considering using to store or process data. For instance, cloud computing services, customer relations management systems or publicity organisations.
- Where necessary, working with other staff and volunteers to ensure communication and other initiatives abide by data protection principles.
- Addressing any data protection queries from journalists or other media outlets.
- Producing and/or providing training and guidance to all staff and volunteers.
- Drafting any data protection statements attached to communications, such magazines, as emails and letters, and on the Mission's website.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees or volunteers can request it from the UK Director.
- France Mission **will provide appropriate training** to all employees and volunteers to help them understand their responsibilities when handling data.
- Employees and volunteers should **keep all data secure**, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared (other than for disaster recovery purposes).

- Personal data **should not be disclosed** to unauthorised people, either within the Mission or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees or volunteers **should request help** from the UK Director or the Trustee responsible for data protection if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Trustee responsible for data protection.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Personal Computers and laptops should be **protected by strong passwords** that are changed several times a year and never shared (other than for disaster recovery purposes).
- If data is **stored on removable media** (for example USB drives, CD's or DVD's), these should be kept locked away securely when not being used.
- USB drives used to store personal data must be **password protected** and preferably encrypted.
- Data should only be stored on **designated drives** and should only be uploaded to an **approved cloud computing services**.
- Personal Computers containing personal data should be **sited in a secure location**.
- Data should be **backed up frequently** and any backups on removable media should be tested annually.
- Data should **never be saved directly** to smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to France Mission unless the Mission can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees and volunteers should ensure **the screens of their computers are always locked** when left unattended in a place to which other persons have access.
- Personal data **should not be shared informally**. In particular, it should not be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The Trustee responsible for data protection can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Where possible, employees and volunteers **should not save copies of personal data to their own computers.** Data accessed in this way should be processed and permanently deleted.

Data accuracy

The law requires France Mission to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort France Mission should put into ensuring its accuracy.

It is the responsibility of all employees and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Employees and volunteers should not create any unnecessary additional data sets.
- All employees, volunteers and trustees should **accept responsibility for data accuracy.** For instance, by confirming a supporter's details when they contact them or by email signatures requesting notification of changes.
- Data should be **updated as soon as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- France Mission will make it **easy for data subjects to update the information** France Mission holds about them.
- It is the responsibility of the Trustee responsible for data protection to ensure **email databases are checked against third party suppression files** regularly and at least annually.

Subject access requests

All individuals who are the subject of personal data held by France Mission are entitled to:

- Ask **what information** the Mission holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the Mission is **meeting its data protection obligations**.

If an individual contacts the Mission requesting this information, this is called a subject access request.
Subject access requests from individuals should be made by email, addressed to the Trustees at services@francemission.org . The Trustees will supply a standard request form, although individuals do not have to use this.
Unless multiple or particularly complex requests are made, individuals will not be charged for a subject access request. The Trustees will aim to provide the relevant data within 14 days.

The Trustees will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, France Mission will disclose requested data. However, the Trustees will ensure the request is legitimate, taking legal advisers where necessary.

Providing information

France Mission aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the Mission has a privacy statement, setting out how data relating to individuals is used by the Mission. This is available on the Mission's website.