



**General Data Protection Regulations
(GDPR)
Policy**

May 2018

1. Introduction

The UK's Data Protection Act 1998 (DPA) and the EU's General Data Protection Regulation (GDPR) are both intended to regulate the processing of "personal data" by individuals and organisations.

Anyone recording, processing or obtaining information about individuals must ensure they are complying with these regulations.

The Mary Frances Trust policy on Data Protection is defined in this document and sets out specific requirements for processing and managing personal data.

Mary Frances Trust is registered as a "Data Controller" under the Data Protection Act.

1.1 General provisions

- This policy applies to all personal data processed by the Charity.
- The Data Controller shall take responsibility for the Charity's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

1.2 Definitions

Data Protection Officer - For the purpose of this document the Data Protection Officer is the person charged with co-ordinating compliance under DPA and GDPR legislation. In practice Mary Frances Trust is not a large enough organisation to have one person dedicated to this task so the role may be shared by various people, but the CEO will take primary responsibility.

Data Controller - Under UK legislation there can only be one "Data Controller" for each registration (or notification) under the DPA. The Data Controller is therefore registered as Mary Frances Trust.

Data Subject - Any individual about whom data is stored or processed.

Personal Data – Information held by Mary Frances Trust about an individual (including clients, supporters, professionals, volunteers, trustees and employees).

1.3 Responsibilities

The following sections describe responsibilities specifically in respect of Data Protection.

1.3.1 Mary Frances Trust Management

Mary Frances Trust Management is responsible for:

- implementing data security controls and policies that are appropriate for ensuring compliance with all relevant UK and EU regulations;
- maintaining the Mary Frances Trust registration with the Information Commissioner's Office;

- ensuring that all employees and volunteers are made aware of their obligations to comply with the policies set out in this document and other related documents.

1.3.2 All Staff, Trustees & Volunteers

All staff, trustees and volunteers are responsible for:

- complying with the policies set out in this document.
- ensuring the confidentiality of all personal data that they have access to.
- ensuring appropriate consent is granted and recorded, as set out in this document and in any procedures, manual issued to them, whenever personal data is collected or utilised;
- reporting any known or possible data breach **immediately** to the CEO.

General Principles of Policy

GDPR and DPA regulations cover everyone about whom you keep personal data. This includes:

- Clients/Service users: People who receive MFT emotional and practical support, clients and family members.
- Employees: Individuals employed by MFT.
- Volunteers: Individuals who provide their time and skills for free and include those who provide emotional and practical support to clients, trustee's, patrons, IT persons, research support and profile raising.
- Members of MFT: who have voter's rights at MFT s AGM and/or receive newsletters from the Mary Frances Trust.
- Supporters- Individuals who support MFT promotional events.
- Donors: Individuals who provide donations and/or legacies to MFT

It is the intention of this policy that Mary Frances Trust will comply with the requirements of both the GDPR and the DPA.

Together, the GDPR and the DPA regulate the "processing" of any information relating to individuals. In the case of Mary Frances Trust this will include: -

- any personal and sensitive information collected and processed in the ordinary course of providing our service – this will include data about clients; referrers, volunteers, professional contacts, trustees and supporters
- any personal and sensitive information collected and processed in relation to staff / employees;
- Any information collected within special categories for the purpose of monitoring and reporting.

The legislation:

- requires organisations to register with the Office of the Information Commissioner if they process personal data
- governs the processing of personal data including 'personal sensitive data'
- allows anyone, about whom you hold personal data, to request to see the personal data held on them; to have that data rectified if it is incorrect or

incomplete; in some circumstances to have the data erased and to restrict how that data is processed or used.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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 considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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 by the GDPR in order to safeguard the rights and freedoms of individuals; and
- 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. NB 2 Please see Data Protection Framework for timescales.

Article 5(2) requires that:

- the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Mary Frances Trust Policy Section

1.4 Registration under the UK Data Protection Act

Mary Frances Trust CEO (or whoever is appointed by them to act on their behalf) is responsible for maintaining Mary Frances Trust's registration under the Data Protection Act and ensuring it is complete and up to date.

1.5 Security

Mary Frances Trust CEO (or whoever is appointed by them to act on their behalf) must ensure appropriate security measures are in place to safeguard personal data.

The primary data storage systems utilised by Mary Frances Trust are operated by third parties – Cloud and Microsoft Corporation (Office 365). Where personal data is processed by a third party, the Data Controller must ensure that appropriate security arrangements are being followed by the third party. The Data Controller should therefore only appoint processors who can provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of data subjects protected. This may be in the form of a written agreement, a letter or e-mail from the third party confirming how data is secured or by undertaking an assessment of the third party as a suitable partner to act in such a role (or a combination of these approaches).

The Data Controller must also ensure that any data held on Mary Frances Trust laptops or desktop computers is adequately secured and staff are aware of their responsibilities in this regard.

1.6 Data Processing

Mary Frances Trust has 4 main purposes for processing personal data:

- **Provision of Mary Frances Trust support service for clients.**
Client data is used by staff and management to ensure that the service provided to clients is appropriate and meets the standards required by the Trust.
- **Fundraising for and Marketing of the service offered by Mary Frances Trust**
Contact details of supporters, volunteers, health professionals, clients and their relatives may be contacted for the purpose of explaining the service offered by the Trust and to support fundraising initiatives.
- **Provision of statistical data.**
Statistical data (which does not normally include personal identifiers) is used to support the management of the service and to support funding from other organisations (such as the Clinical Commissioning Group and Surrey County Council.) that may provide funding for Mary Frances Trust.
- **HR support and staff payroll.**
Staff data is used to support the HR function of Mary Frances Trust.

There are six available lawful bases for processing. The following are most relevant to Mary Frances Trust

1.6.1 Types of Data we collect

The personal information we collect is used primarily to enable us to provide the specific service you require, and for the purpose of reporting to stakeholder and funders.

Personal information can include the following:

- title, forename and surname and gender;
- personal e-mail addresses
- personal contact details including postal address; telephone number(s),
- marital status
- date of birth
- Medical information, and medical contacts

Personal information also includes special categories of personal data. This is data about your racial or ethnic origin, religious or philosophical beliefs, genetic data, data concerning your health, sexual orientation, is or was armed forces.

1.7 Consent

This will be the usual lawful basis for processing client and volunteer data to enable the:

provision of Mary Frances Trust service;
collation of statistical data;
the distribution of fundraising and other direct marketing materials.
When fundraising and direct marketing materials are distributed the recipients will be given the opportunity to “opt out” of future mailings.

1.7.1 Contract

This will be the usual lawful basis for processing staff data for the payment of salaries and related tasks.

1.7.2 Lawful, fair and transparent processing

- To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
- The Register of Systems shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

1.7.3 Legitimate Interests

This will be the usual lawful basis for processing data relating to all types of related parties for the:

- the distribution of newsletters to professionals
- the distribution of newsletters to beneficiaries, supporters and members.

When newsletters are distributed the recipients will be given the opportunity to “opt out” of future mailings.

1.8 Right to be Informed / Privacy Notices

1.8.1 Consent

As a general principal, Mary Frances Trust will obtain consent whenever it collects personal data directly from the data subject.

When data are collected from a third party (such as referrers) the data subject will be informed of the categories of personal data received and this will be done within a reasonable period of having obtained the data (normally within one month). The data subject will be asked to consent to the data being recorded by Mary Frances Trust.

Personally Collected Consent

In all cases where consent is requested personally, the data subject will be asked to sign a "Privacy Notice" which includes:

- Why the data is being collected.
- How it will be used, with an opt-in / opt-out option for each purpose.
- Who it will be shared with (if required).
- The right to opt-out at any time.

Impersonally Collected Consent

Where data is collected via an on-line form, e.g. via Mary Frances Trust website, Mary Frances Trust will include a "tick box" to indicate consent and access to an appropriate "Privacy Notice" (*appendix 2*) that can be accessed by the data subject.

1.8.2 Disclosure

If disclosure to another recipient is envisaged (for example if a client is being signposted to another organisation), the data subject must give consent before the data are disclosed.

1.8.3 Subject Access Rights

Under the GDPR, individuals have the right to obtain access to their personal data so that they are aware of and can verify the lawfulness of the processing

In normal circumstances Mary Frances Trust will provide a copy of the data held at the earliest possible time but no later than within 1 month of receiving the written request. In line with the requirements of the GDPR there will normally be no charge made for providing the data.

Persons making an enquiry or requesting access to their data will be provided with a subject access request form (*see Appendix 1*). This form will:

- Request the information required to locate the data requested e.g.- an individual should provide their full name; the nature of their relationship with Mary Frances Trust (e.g. ex-member of staff); the approximate dates of that relationship; any other information which may assist in locating the data.
- Request Proof of Identity to be provided.

- Indicate that the response will be provided promptly and in any event within 30 days of receiving the required information.

1.8.4 Right to Rectification / Erasure / Restrict Processing / Object Complain

1.8.5 Rectification

If Mary Frances Trust is advised by any data subject that the data held about them is incorrect it will be corrected at the earliest opportunity and no later than 1 month after receiving the notification. If the data has been disclosed to any third party, then that third party will also be informed of the correction.

1.8.6 Erasure

If Mary Frances Trust is advised by any data subject that the data held about them should be erased, it will be erased or anonymised at the earliest opportunity and no later than 1 month after receiving the notification. If the data has been disclosed to any third party, then that third party will also be informed of the requirement for it to be erased.

Note: In some circumstances this could result in Mary Frances Trust no longer being able to provide its service to a client. In such circumstances the client will be advised accordingly.

1.8.7 Restrict Processing / Object

If Mary Frances Trust is advised by any data subject that the data held about them should no longer be used for a specific purpose, this will be recorded on their record and that purpose will be discontinued. This is most likely to occur in relation to direct marketing or similar processes.

1.8.8 Right to Complain

All MFT data subjects have the right to lodge a complaint with the UK's Information Commissioner if they consider that we have infringed applicable data privacy laws when processing their personal data. Information Commissioner's Office can be contacted using the following link: <https://ico.org.uk/>

1.9 Transfer of Personal Data Overseas

Mary Frances Trust does/will not transfer personal data overseas, except for information stored on Cloud and MailChimp.

1.9.1 Data Breaches and Reporting

The GDPR introduces a duty on all organisations to report certain types of data breach to "the relevant supervisory authority". In some cases, organisations will also have to report certain types of data breach to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This means that a breach is more than just losing personal data.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, the Charity

shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](#)).

For example, Mary Frances Trust could be responsible for a personal data breach if a client's record is inappropriately accessed.

A data breach only has to be notified to the relevant supervisory authority where 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.

This has to be assessed on a case by case basis. For example, Mary Frances Trust would need to notify the relevant supervisory authority about a loss of client details where the breach leaves individuals open to identity theft or significant loss of confidentiality. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

A notifiable breach, in line with MFT breach reporting template and procedure must be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

At the time of writing the "relevant supervisory authority" for Mary Frances Trust will be The Charity Commission for England and Wales.

It may also be necessary to report the breach to the Information Commissioner's Office. Their advice should be sought accordingly.

Use of Computer Systems and Manual Systems

1.10 Microsoft Office

Office 365 is a cloud-based file storage system used by the Trust as the main depository for all general files (documents, spreadsheets photographs etc.) It is therefore possible that personal data may be held and processed using data held in this system (this is particularly possible in the case of spreadsheet-based data). It should be noted that the Cloud is kept outside of the UK

Therefore, care must be taken with data in Microsoft Office ensure that it is:

- stored safely;
- deleted when no longer required;
- not transferred outside of the organisation without appropriate consent.

The same approach when transferring personal data files via email between members of the organisation.

1.11 Website

Mary Frances Trust public website (www.maryfrancestrust.org.uk) is not used to process data however it does contain some personal data and is used to collect some personal data.

Therefore the website will:-

- incorporate a suitable “Privacy Notice” document that can be accessed by any user;
- include a pointer to the “Privacy Notice” in any on-line forms that collect personal data;
- include “opt-in / opt-out” and / or “consent” tick boxes as appropriate on on-line forms that collect personal data;
- include an appropriate “Privacy Notice” on any downloadable forms that may be used collect data off-line.

Information may be collected about Internet Service Provider, operating systems, browser types, domain names, the Internet Protocol (IP) address (or other electronic Internet-enabled device), visiting times, websites that referred people to us, the web pages requested and the date and time of those requests.

Our collection of website use information may also involve the use of cookies to track personal data.

1.12 E-mail Systems

Email is not a totally secure medium and therefore care must be used if transmitting personal or confidential information. Attachments containing confidential information must be protected with a password which is passed to the recipient in a separate email or verbally. Egress will be used to send sensitive personal data.

1.13 Text and Answer Machine

All Messages by these mediums will be kept in the strictest confidence and by the relevant member of staff until the enquiry has been dealt with. Once this has been done, the message will be deleted. No text or answer machine communication will be kept longer than necessary.

1.14 Halo Database

The Halo Database is the main data processing system utilised by MFT and holds client data.

Great care must be taken when extracting personal data from Halo to ensure that it is:

- stored safely;
- deleted when no longer required;
- not transferred outside of the organisation without appropriate consent.

If data is transferred by email to members of the organisation, for example in the form of a spreadsheet or word-processing document, it should be secured by using a password to lock the document and the password should be passed on in a separate email. Halo is used to store data and produce vital statistics.

1.15 Mail Chimp

Mail chimp is the platform used to distribute information such as the monthly newsletters, and information about activities, groups and courses.

To receive this information users will need to 'opt in' to the service and as such give permission for their information to be used for the stated purpose, and go on the distribution list

All users have the right to 'opt out' after opting in

The information stored within includes email addresses and names.

Information may be collected about Internet Service Provider, operating systems, browser types, domain names, the Internet Protocol (IP) address (or other electronic Internet-enabled device).

2. Appendix 1 – Data Subject Access Request Form

	MFT Personal Data Access Request
Full Name:	
Address	
Relationship to Mary Frances Trust	Ex Staff / Volunteer / Client / Other <i>(Delete as appropriate)</i>
Approximate Dates of Relationship	From: To:
Please describe the nature of the data requested	

Please provide one form of identification showing your current address, from the following list:

1. Photocopy of Passport
2. Photocopy of Driving Licence
3. Photocopy of Utility Bill

Signed: _____

Date: _____

APENDIX 2 – PRIVACY NOTICE

As a charitable organisation, providing services to people with any emotional or mental health issues, Mary Frances Trust (MFT) needs to know certain things about you.

Keeping your personal information safe is a responsibility we take very seriously and in this privacy notice we spell out exactly what you can expect from us when it comes to your information.

If you are interested in knowing more about how we look after the information you've given us, you can find it here in our General Data Protection Regulations (GDPR) Policy: [add link here](#)

WHY DO WE NEED YOUR INFORMATION

There are three reasons why we collect information about you:

- To be able to provide tailored and best suited services to your needs.
- To provide you with information about MFT and give you choice to select services that work for you and that you find interesting.
- To be able to evidence to our funders and commissioners that we provide not only good quality services but also that they are a value for money.

WHAT INFORMATION DO WE COLLECT

We never collect more information than absolutely required and here is what we currently store on our secure database: your name; date of birth; your address; your house and/or mobile telephone number; email address; important information about your emotional/mental and physical health; next of kin; GP and other professionals details – to help us working together and provide better support for you.

HOW DO WE GET INFORMATION ABOUT YOU

- Most of the information about you we collect when you (or the person that refers you to our service) fill in on the referral form.
- If you contact us via email, post or telephone, we may keep a record of that contact
- When you visit our website www.maryfrancestrust.org.uk, some information may be stored to enhance your experience and help you navigate the site, but also to help us make our website user-friendly and useful. For more details on information collected through our website, please check our Website and Cookies Policy here: [add link here](#)

WHO DO WE SHARE YOUR INFORMATION WITH

Most importantly, we will never share any information we hold about you for any marketing purposes.

We may however share relevant information with your GP or other professionals providing support to you.

We provide anonymised statistics about people we provided services for to our funders and commissioners.

HOW LONG DO WE KEEP YOUR INFORMATION

We review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations. As a baseline, we will keep basic information about you for 6 years but not longer than necessary.

HOW DO WE KEEP THE INFORMATION SAFE

We always ensure there are appropriate controls in place to protect your personal details. Most of the information we hold about you is stored on our web-based database and on the Cloud.

If we store any personal information on any of our electronic devices (e.g. on the laptop), we make sure the information is appropriately encrypted.

We do comprehensive checks on companies that may be processing our data and sign contracts that set out our expectations and requirements, especially how they manage the personal data they collect on our behalf, or have access to.

HOW CAN YOU SEE IT

You have the right to see the information we hold about you and ask us to amend any incorrect information. You also have the right to ask us to delete information we hold about you or stop using it altogether.

You can do all of the above by:

- Telephone: 01372 375 400
- Email: info@maryfrancestrust.org.uk
- Post: Mary Frances Trust, 23 The Crescent, Leatherhead, Surrey, KT22 8DY