

UK GDPR POLICY

| Review | Date | Description of Change | Planned Review Date |
|--|--------------------------------|-----------------------|---------------------|
| Julie Marriott – CEO | 4 th October 2021 | Review of content | October 2022 |
| John Musson - Trustee | 17 th November 2022 | Review of Content | November 2023 |
| Rob Jacques Head of Finance & Compliance | December 2023 | Clarification of DPO | December 2024 |
| | | | |

1. Purpose

Family Gateway is required to keep certain information about its staff, trustees, volunteers, and service users to enable it to run efficiently and effectively for the benefit of those it serves. Family Gateway is therefore committed to protecting the privacy and security of personal information.

This policy describes how we collect and use personal information in accordance with the UK General Data Protection Regulation (UK GDPR).

Family Gateway collects, uses and is responsible for certain personal information. When we do so we are regulated under the UK GDPR which applies throughout the United Kingdom, and we are responsible as 'controller' of that personal information for the purposes of those laws.

2. Definition of Key Terms

Personal Data – means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

Sensitive Personal Data – can include information about race, ethnic origin, criminal convictions and offences, sexual orientation, or religious beliefs.

Data Controller (DC) – The DC is responsible for implementing appropriate technical and organisational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the **GDPR**. These measures may include implementing an appropriate privacy policy

Data Protection Officer (DPO) – The DPO ensures, in an independent manner, that an organisation applies the laws protecting individuals' personal data.

Information Commissioner's Office (ICO) – The ICO is the independent regulatory office in charge of upholding information rights in the interest of the public.

3. The Seven Principles

The UK GDPR sets out seven principles for the lawful processing of personal data. Processing includes the collection, organisation, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of personal data. Broadly, the seven principles are:

a. Lawfulness, fairness and transparency

In practice this means you must:

- *have legitimate grounds for collecting and using the personal data;*
- *not use the data in ways that have unjustified adverse effects on the individuals concerned;*
- *be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;*
- *handle people's personal data only in ways they would reasonably expect; and*
- *make sure you do not do anything unlawful with the data.*

b. Purpose limitation

In practice this means you must:

- *be clear from the outset about why you are collecting the personal data and what you intend to do with it;*
- *comply with the Regulation's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;*
- *comply with what the Regulation states about notifying the ICO; and*
- *ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose the new use or disclosure is fair.*

c. Data minimisation

In practice, it means you should ensure that:

- *you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual;*
- *you do not hold more information than you need for that purpose; and*
- *you should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information, but no more. This is part of the practice known as "data minimisation".*

d. Accuracy

To comply with these provisions, you should:

- *take reasonable steps to ensure the accuracy of any personal data you obtain;*
- *ensure that the source of any personal data is clear;*
- *carefully consider any challenges to the accuracy of information; and*
- *consider whether it is necessary to update the information.*

e. Storage limitation

In practice, it means that you will need to:

- *review the length of time you keep personal data;*
- *consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;*
- *securely delete information that is no longer needed for this purpose or these purposes;*
- *update, archive or securely delete information if it goes out of date; and*
- *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 ('storage limitation').*

f. Integrity and confidentiality (security)

In practice, it means that we will:

- *process information in a manner that ensures appropriate security of the personal data;*
- *protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

g. Accountability

We take responsibility for complying with UK GDPR, at the highest management level and throughout Family Gateway. We keep evidence of the steps we take to comply with UK GDPR. We also put in place appropriate technical and organisational measures such as;

- *adopting and implementing data protection policies;*
- *putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;*
- *maintaining documentation of our processing activities;*
- *implementing appropriate security measures;*
- *recording and, where appropriate, reporting any security breaches;*
- *appointing a Data Protection Officer (DPO);*
- *we review and update our accountability measures at appropriate intervals.*

4. Rights of Data Subjects

Under the UK GDPR individuals have a number of important rights. Under certain circumstances, individuals have the right to:

- **Request access** to personal information and to certain other supplementary information that this Policy is already designed to address;
- **Request correction** of the personal information that we hold. This enables individuals to have any incomplete or inaccurate information we hold corrected;
- **Request erasure** of personal information. This enables individuals to ask us to delete or remove personal information where there is no good reason for us continuing to process it. They also have the right to ask us to delete or remove personal information where individuals have exercised their right to object to processing (see below).
- **Object to processing** of personal information where we are processing your personal information for direct marketing purposes.
- **Object to decisions** being taken by automated means which produce legal effects concerning or similarly significantly affect individuals;
- **Object in certain other situations** to our continued processing of your personal information;
- **Request the transfer** of your personal information to another party.

5. Principles of this Policy

Family Gateway staff, Trustees and Volunteers who process or use any personal information in the course of their duties must ensure that these principles are followed at all times.

6. Data Protection Officer

Family Gateway has appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice and Family Gateway Board Members are ultimately responsible for the Policy's implementation. However, Family Gateway has designated the GDPR Lead (Head of Finance & Compliance) to deal with any day-to-day matters arising from the implementation of the UK GDPR Policy.

7. Personal Data Use

To ensure that this happens, Family Gateway has drawn up this policy. There are two main groups to accommodate within the policy:

- *Service Users*
- *Volunteers/Staff/Trustees*

8. Personal Data Relating to Service Users

Family Gateway obtains contact details (names, addresses and telephone numbers) and other details from service users. This data is obtained, stored and processed solely to assist staff and volunteers in the efficient running of the service requested by the service user and on occasion, it is shared with commissioners and other agencies. Personal details supplied by service users are not used to send marketing material or Family Gateway newsletters, unless prior consent is obtained.

9. Personal Data Relating to Staff, Volunteers and Trustees

During the course of duties with Family Gateway, volunteers, staff, and trustees will be dealing with information such as names, address, and telephone numbers of staff, volunteers, trustees, donors and other details of service users. Sensitive information may be overheard while working at Family Gateway.

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

ASSOCIATED DOCUMENTS AND PROCEDURES

This policy supplements the following:

- Data Protection Policy
- Privacy Policy
- Social Media Policy
- Confidentiality Policy
- Information Governance Policy