Data Protection Policy

Family for Every Child (Family) is committed to complying with privacy and data protection laws including the European General Data Protection Regulation (GDPR) and any related legislation which applies in the UK, without limitation, any legislation derived from the UK Data Protection Bill 2017; the European Privacy & Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, European E-Privacy Regulation 2017/0002; and all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the UK Information Commissioner's Office (ICO) or any other supervisory authority.

This policy sets out how we seek to protect individual's personal data and ensure that all individuals within the scope of this policy (see below) understand the rules governing their use of personal data to which they have access in the course of their work.

We hold personal data about our employees - current, past and prospective, consultants, members, supporters, suppliers and other individuals for a variety of organisational purposes. This personal data must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Scope

This policy applies to anyone who has access to or handles personal data obtained on behalf of Family. You must be familiar with this policy and comply with its terms. Failure to comply with this Policy could expose Family to enforcement action by the UK Information Commissioner's Office (ICO), and could create negative publicity for Family if any breach is made public. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

Who is responsible?

Family's **Data Protection Officer** (DPO) is appointed on an annual basis and the name of the DPO is listed on the Website and is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about this policy should be referred in the first instance to the DPO who can be contacted at dataprotection@familyforeverychild.org.

Definitions of data protection terms

The following terms will be used in this policy and are defined below:

Data Subjects include all living individuals about whom we hold personal data, for instance an employee or supporter. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal Data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance review). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data Controllers are the people who, or organisations, which decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. Family is the data controller of all personal data that we manage in connection with our work and activities.

Data Processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

European Economic Area includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

ICO means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

Processing is any activity that involves use of personal data, whether or not by automated means.

It includes but is not limited to:

- collecting
- recording
- organising
- structuring
- storing
- adapting or altering
- retrieving
- disclosing by transmission
- disseminating or otherwise making available
- alignment or combination
- restricting
- erasing or destruction of personal data

Sensitive Personal Data (which is defined as 'special categories of personal data' under the GDPR) includes information about a person's:

- racial or ethnic origin
- political opinions
- religions, philosophical or similar beliefs
- trade union membership
- physical or mental health or condition
- sexual life orientation
- genetic data
- biometric data
- such other categories of personal data as may be designated as 'special categories of personal data' under the Legislation

Responsibilities

The **Data Protection Officer** is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff and those included in this policy
- Answering questions on data protection from staff, Board members and other stakeholders
- Ensuring Family responds to individuals such as employees and supporters who wish to know which data is being held on them
- Checking and approving with third parties that handle Family's data any contracts or agreement regarding data processing
- Ensuring the responsibilities below are delegated to an appropriate staff member including where applicable compliance with UK statutory data retention periods:

IT

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Ensuring security hardware and software is checked regularly to ensure it is functioning properly
- Ensuring third-party services, such as cloud services Family is considering using to store or process data, are properly researched

Fundraising and Communications

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from supporters, target audiences or media outlets
- Coordinating with the DPO to ensure all fundraising and marketing initiatives adhere to data protection laws and Family's Data Protection Policy
- Ensuring Family's Privacy Policy is consistent with the principles of the DPA

HR

- Ensuring the use and storage of staff, consultants and candidates' data and information is consistent with the employment relationship and the principles of the DPA

Finance

- Ensuring the use and storage of details of individuals who Family makes payments to by third parties, is consistent with the principles of the DPA

Member relations

- Ensuring the use and storage of details of individuals from member organisations is consistent with the principles of the DPA

Data protection principles

Anyone processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles and show that we comply, in respect of any personal data that we deal with as a data controller. Personal data should be:

1. **Processed fairly, lawfully and transparently**
   The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

   To comply with this principle, every time we receive personal data about a person directly form that individual, which we intend to keep, we need to provide that person with 'the fair processing information'. In other words we need to tell them:
   a. the type of information we will be collecting;
   b. who will be holding their information i.e. Family;
   c. why we are collecting their information and what we intend to do with it;
   d. the legal basis for collecting their information;
   e. if we are relying on legitimate interests as a basis for processing and what those legitimate interests are;
   f. whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;
   g. the period of which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;
   h. details of people or organisations with whom we will be sharing their personal data;
   i. if relevant, the fact that we will be transferring heir personal data outside the EEA and details of relevant safeguards; and
   j. the existence of any automated decision-making including profiling in relation to that personal data.

Where we obtain personal data about a person from a source other than the person his or her self, we must provide that individual with the following information in addition to that listed above:

a. the categories of personal data that we hold; and
b. the source of the personal data and whether this is a public source.

2. **Collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with these purposes**
   This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed beforehand.

3. **Adequate, relevant and limited to what is necessary for the purpose for which it is held, and**
4. **Accurate and, where necessary, kept up to date**
   Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

5. **Not kept longer than necessary**
   This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed.

6. **Processed in a manner that ensures appropriate security of the personal data**
   We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

   When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands. When we are dealing with sensitive personal data more rigorous security measures are likely to be needed.

The following security procedures and monitoring processes must be followed in relation to all personal data processed by Family:

- encryption of personal data
- process for regularly testing, assessing and evaluating effectiveness of security measures
- backing up data
- paper documents should be shredded, memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required
- personal data must always be transferred in a secure manner
- other measures to ensure confidentiality, integrity, availability and resilience of processing systems
- staff must keep data secure when travelling or using it away from their normal place of work

Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of Family needs to be aware of these rights. They include (but are not limited to) the right:

a. to request a copy of any personal data that we hold about them as well as a description of the type of information that we are processing , the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored
b. to be told, where any information is not collected from the person directly, any available information as to the source of the information
c. to be told of the existence of automated decision-making
d. to object ot the processing of data where the processing is based on either the conditions of public interest or legitimate interests
e. to have all personal data erased unless certain limited conditions apply
f. to restrict processing where the individual has objected to the processing
g. to have inaccurate data amended or destroyed; and
h. to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

Transferring data outside the EEA

The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected.

The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, but this list may be updated.

As such personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA it will be necessary to enter into an EC-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under GDPR that apply to the transfer of personal data outside the EEA.

The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US< although specific advice should be sought from the Data Protection Officer before transferring personal data to organisations in the US.

Processing sensitive personal data

On some occasions we may collect information about individuals that is defined by the GDPR as special categories of personal data and special rules will apply to the processing of this data.

Notification

We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR we will consult with the ICO where necessary when we are carrying out 'high risk' processing.

We will report breaches (other than those which are unlikely to be a risk to individual) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individual.

Monitoring and review of this policy

This policy is reviewed annually by our Board to ensure that it is achieving its objectives.