Families First Data Protection Policy

Preface

All new staff and trustees must read this policy as it gives important information about the organisation's policy on data protection, responsibilities of staff and trustees, and details certain important principles and processes.

New staff and trustees should sign and confirm they have read and understood the policy as part of their induction. Current staff should sign and confirm they have read and understood any updates to the policy as notified to them after updates have been made.

1. Introduction and scope

1.1 Families First takes its responsibility concerning the security and privacy of personal information, very seriously.

1.2 We collect and process personal information (also referred to as data) about job applicants, current and former staff, temporary and agency workers, contractors, interns, volunteers and apprentices, suppliers, service users, partners and funders.

1.3 This document sets out how we comply with our data protection obligations.

1.4 Families First Manager (Morag Coleman) is responsible for data protection compliance within the organisation, known as the Data Protection Officer (DPO). Any questions or comments should be addressed to her via email manager@familiesfirststandrews.org.uk

1.5 All new staff and trustees must read this policy as it gives important information about the organisation's policy on data protection, responsibilities of staff and trustees, and details about important principles and processes.

1.6 New staff and trustees should sign and confirm they have read and understood the policy as part of their induction.

1.7 Current staff should sign and confirm they have read and understood any updates to the policy as notified when updates have been made.

2. Definitions

Data subject	A living identified or identifiable individual, about whom we hold personal data.
Personal data	Any information relating to an individual who can be identified (directly or indirectly) from that information.
Processing information	Collecting, storing, amending, disclosing and/or destroying information.

Special categories of personal data	Special categories of personal data or 'sensitive personal data', means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Criminal records data	Information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data protection principles

3.1 Families First will follow the data protection principles under the Data Protection Act (2018) relating to the processing of personal data which is used, stored or processed. The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes, and will not be processed in a way that is incompatible with those purposes.
- Processed in a way that is adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that inaccurate personal information is deleted or corrected without delay.
- Kept for no longer than is necessary for the purposes for which the information is processed.
- Processed in a manner that ensures appropriate technical and organisational measures are taken to keep the data secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

3.2 We will not transfer personal data to outside the EEA without appropriate safeguards being in place.

3.3 We will make personal data available to data subjects and will allow data subjects to exercise certain rights in relation to their personal data.

4. Basis for processing personal information

4.1 We tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices - see section 6 below. We will not process personal data of individuals for other reasons.

4.2 Where we process special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the following policy on special categories of data and criminal records data:

- We will only process special category data that is necessary for the purposes of our obligations in employment law, for example in regard to monitoring and managing sickness absence.
- We will only use this data for purpose in which it is collected.
- We will process criminal record data in the vetting of individuals as part of our employment and recruitment processes.
- We will update HR related personal data promptly when you advise that your information has changed or is inaccurate.
- Personal data gathered during employment, or other type of contract, is held in your personnel file (in hard copy and electronically) in our HR systems.

5. Record keeping

5.1 Families First will keep records of all personal data in line with our retention of records procedure at Appendix A.

5.2 Following the retention period all hard copy written records will be securely destroyed and all electronic records will be deleted from our computer systems.

5.3 Basic data will be recorded for the purposes of writing references or future safeguarding enquiries including:

5.4

- End of service child data record.
- End of service adult data record.
- End of service staff/volunteer record.

6. Privacy notices

6.1 Families First have a number of Privacy Notices informing different groups of people about the personal data we collect and hold on them and how they can expect their personal information to be used and for what purposes the privacy notices cover the following groups:

6.1.1 Service Users
6.1.2 Members, Volunteers & Funders
6.1.3 Employees
6.1.4 Recruitment
6.1.5 Web site users
6.1.6 Social media – see paragraph 6.2 below.

6.2 **Facebook Privacy Notice** – This notice appears on our Facebook page:

“Families First would like you to know that we cannot guarantee your privacy when using our Facebook pages. We do analyse some of the data gathered for our own purposes such as to see how many people are using our pages and how we can improve our reach and business.

We will not share your personal data with third parties unless we are concerned about your wellbeing through your posts; in that instance we will try and contact you before taking any action.

Please be aware that others can see anything you post on our pages."

7. Responsibilities

7.1 All staff have responsibilities under the Data Protection Act not to disclose personal information outside of Families First or use it for their own purposes.

7.2 All staff should ensure that their personal data is kept up to date by informing the Office Manager of any change in circumstances affecting the personal data we process such as change of personal details, bank account, etc.

7.3 Staff, volunteers and others may have access to personal data in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, we rely on them to help meet our data protection obligations. "Others" include ICT consultant (JEM Computing), HR consultant (Caroline Rochford Consulting), accountants (Henderson Black), bank (BoS), database consultant (Mike Martin).

7.4 Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes.
- Not to disclose data except to individuals (whether inside or outside of the organisation) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
- To adopt appropriate security measures (such as encryption or password protection) to secure personal data, or devices containing that data or used to access personal data, when working from home and elsewhere.
- Not to store personal data on local drives or on personal devices that are used for work purposes.
- To report data breaches of which they become aware to the Office Manager immediately.

7.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our Disciplinary Procedure.

7.6 Significant or deliberate breaches of this policy, such as accessing employee or service user data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

8. Individual rights - Subject Access Requests (SAR)

8.1 Individuals have the right to gain access to information kept about them – this is known as subject access.

8.2 Subject access requests for children should be given the same amount of due consideration as an adult.

8.3 If you make a subject access request we will tell you:

- Whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you.
- To whom your data is, or may be, disclosed to, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- How long your personal data is stored (or how that period is decided).
- Your rights to rectification or erasure of data, or to restrict or object to processing.
- Your right to complain to the Information Commissioners Office if you think we have failed to comply with your data protection rights.

8.4 We will also provide you with a copy of the personal data undergoing processing. This will be in electronic form if you have made a request electronically unless you agree otherwise.

8.5 To make a subject access request, you should send your request to the Manager via manager@familiesfirststandrews.org.uk

8.6 In some cases, we may need to ask for proof of identification before the request can be processed.

8.7 We will normally respond to a request within a period of one month from the date it is received.

8.7.1 In some cases, if we are processing large amounts of the individual's data, we may respond within three months of the date the request is received.

8.7.2 We will write to you within one month of receiving the original request to tell you if this is the case.

8.8 If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it.

8.8.1 A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded.

8.8.2 If an individual submits a request that is unfounded or excessive, Families First will notify them that this is the case and whether or not we will respond to it.

8.9 Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

9. Individual rights – other rights

9.1 You should refer to the relevant data protection privacy notice for the grounds on which we process your personal data. As a data subject you can:

- Access and obtain a copy of your data on request.

- Ask us to change incorrect or incomplete data.
- Ask us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing.
- Object to the processing of your data where we are relying on our legitimate interests as the legal ground for processing.
- Ask us to stop processing data for a period if the data is inaccurate or there is a dispute about whether or not your interests override our legitimate grounds for processing that data.
- Withdraw consent to our processing your personal data at any time.

9.2 If you would like to exercise any of these rights, please contact our Manager manager@familiesfirststandrews.org.uk

9.3 If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner.

9.4 Please note that we do not have to erase data that we need to comply with our statutory obligations, or where it is necessary to establish or defend legal claims.

10. Information security

10.1 Families First take the security of all personal data very seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure that data is only accessed by those who need to use the data in the proper performance of their duties.

10.2 Electronic devices used to access data are password protected. We use appropriate technical measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10.3 For those who are opting into our mailing list or subscribing to our newsletters – the basis for processing your data is consent i.e. you have given clear and informed consent by opting in to receiving our newsletter. You may, at any time, unsubscribe and we will remove you from our mailing list.

10.4 Where we engage third parties to process personal data as part of their contract with us, we ensure that appropriate security arrangements are detailed in a specific contractor's agreement.

10.5 Always seek permission in writing to use other people's stories or names in a public arena.

11. Access to confidential and sensitive information

11.1 All information and records held on service users, staff, trustees, and volunteers are held securely with restricted access to authorised personnel as follows:

- PVG certificates – named signatories only.
- Children's records – staff and designated volunteers only (unless requested through a hearing or court process).
- Adult records - staff and designated volunteers only (unless requested through a hearing or court process).

- Volunteer records - staff only.
- Staff records – Manager, named Trustee and Office Manager only.
- Trustee's records – Manager, named Trustee and Office Manager only.
- Job application forms – personnel named for the recruitment process only.
- Risk assessments – all.
- Service evaluations – all.
- Financial records – Trustees and designated staff.

12. Data breaches

12.1 If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will inform the Information Commissioner's Office within 72 hours of discovery.

12.2 We will record all data breaches regardless of their impact on the data subject.

12.3 If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures taken.

12.4 Families First Manager will ensure that training is given to all staff and that the processes for recording data breaches is regularly used, reviewed and updated.

13. Training

13.1 Families First will ensure that staff are adequately trained during their induction period regarding their data protection responsibilities.

13.2 Ongoing training will be provided to all staff and volunteers when this policy is updated and on practicing how to manage a data breach.

Appendix A

Table of retention periods

Type of information	Retention period	Terms of Reference
Accounting records- Maternity, paternity, payroll, benefit records etc	At the end of the sixth financial year.	HMRC
Furlough letters	5 years.	
LEADER in Fife – European Commission funding 2011	We can destroy the files in 2025.	
Donor records of interest	Kept and archived for historical purposes.	
Annual reports, reports of interest.	Kept and archived for historical purposes.	
Staff, volunteers, service user information summary data sheet	Indefinitely.	In light of historical child abuse, adoption, police and fostering enquiries basic information will be retained.
Service User personal records	One year following end of service unless there has been an incident. All records where an incident has been recorded will be kept until the child reaches 25 years.	
PVG Certificates	Will be destroyed 3 months after a recruitment decision has been made.	Disclosure Scotland guidance – Basic PVG ID numbers and dates will be recorded in the folder held in the admin filing cabinet.
Criminal record checks	Deleted promptly after the information has been verified.	

Type of information	Retention period	Terms of Reference
Staff personnel records	Held for the duration of employment and for seven years after the person has left.	Eligibility to work in the UK records – retained 2 years after the staff member has left the company.
Staff personnel records where an incident has been recorded. Any records which may be required to prepare for, or defend, a legal claim.	Until the legal process has been completed.	
Health & Safety records	Up to 10 years depending on the type of record. Until the child reaches 25.	
Volunteer personnel records (including trustees)	Retain for six months after their date of leaving.	
Job applications	Six months following a recruitment decision.	
Risk assessments	Destroyed once a revised RA document has been produced.	
Service evaluations	Destroyed one year after data has been analysed and recorded.	
Time sheets, session registers	One year after statistical analysis has been completed.	
Right to work checks	2 years after the staff member has left.	