

Families First Data Protection Policy

Preface

All new staff and trustees must read this policy as it gives important information about:

- The data protection principles with which Families First must comply.
- What is meant by personal information (or data) and sensitive personal information (or data).
- How Families First gather, use, store and (ultimately) destroy personal information and sensitive personal information in accordance with the data protection principles.
- Where more detailed privacy information can be found, e.g. about the personal information we gather and use about individuals, how it is used, stored, who it is shared with, for what purposes and the steps taken to keep that information secure and for how long it is kept; additional information on this can be found in the various Privacy Notices linked to this Policy.
- Your rights and obligations in relation to data protection.
- The consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to the Office Manager.

1. Introduction

- 1.1** Families First takes the security and privacy of personal information very seriously.
- 1.2** Families First gathers, uses and stores data about many people in the course of its business and in the delivery of its services. We do this to manage our relationship with the people we have contact with.
- 1.3** Families First has a duty to notify service users, staff and volunteers about this Policy.
- 1.4** Families First obtains, uses and stores personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices, suppliers, customers and service users, partners and funders, for a number specific lawful purposes, as set out in Families First's Privacy Notices.
- 1.5** This Policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce, service users and others.
- 1.6** The purpose of this Policy is to ensure that staff, volunteers and others working with or for Families First understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.
- 1.7** Families First is committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce and others, and how (and when) we delete that information once it is no longer required.

1.8 Families First Manager (Morag Coleman) is responsible for data protection compliance within the organisation. If you have any questions or comments about the content of this policy or if you need further information, you should contact her by phone or email at:

- 01334 208086
- manager@familiesfirststandrews.org.uk

2. Scope

2.1 This Policy applies to the personal information of job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices, suppliers, service users, partners and funders and any other third parties we have connections with.

2.2 Staff should refer to Families First's various privacy notices and other relevant policies such as Confidentiality, IT, Internet and Computer Use, Retention of Records.

2.3 Families First will review and update this Policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policies to staff before they are adopted.

3. Definitions

| | |
|------------------------------|--|
| Criminal records information | Means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures. |
| Data breach | Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. |
| Data subject | Means the individual to whom the personal information relates. |
| Personal information | Sometimes known as personal data, means information relating to an individual who can be identified (directly or indirectly) from that information. |
| Processing information | Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it. |
| Pseudonymised | Means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual. |

| | |
|--------------------------------|--|
| Sensitive personal information | Sometimes known as '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. |
|--------------------------------|--|

4. Data protection principles

4.1 Families First will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner.
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes.
- We will only process the personal information that is adequate, relevant and necessary for the relevant purposes.
- We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.
- We will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed.
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. Basis for processing personal information

5.1 In relation to any processing activity Families First will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 Review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, such as:

- The data subject has consented to the processing.
- The processing allows Families First to deliver services to individuals.
- The processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.
- The processing is necessary for compliance with a legal obligation to which Families First is subject.

- The processing is necessary for the protection of the vital interests of the data subject or another natural person.
 - The processing is necessary for the purposes of legitimate interests of Families First or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject, see section **5.2** below.
- 5.1.2** Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis and that there is no other reasonable way to achieve that purpose.
- 5.1.3** Families First will document the decision as to which lawful basis applies, to help demonstrate compliance with the data protection principles.
- 5.1.4** Include information about both the purposes of the processing and the lawful basis for it in our relevant Privacy Notices (appendix A-E).
- 5.1.5** Where sensitive personal information is processed, also identify a lawful special condition for processing that information (see section **6.2.2** below) and document it.
- 5.1.6** Where criminal offence information is processed Families First will identify a lawful condition for processing that information and document it.
- 5.2** When determining whether Families First's legitimate interests are the most appropriate basis for lawful processing, we will:
- 5.2.1** Conduct a Legitimate Interests' Assessment (LIA) (appendix F) and keep a record of it to ensure that we can justify our decision. A LIA is a process where Families First establish why they have selected Legitimate Interest as the basis for processing someone's information. The Information Commissioner's Office (ICO) sets out three elements to this process:
- Identify a legitimate interest.
 - Show that the processing is necessary to achieve it.
 - Balance it against the individual's interests, rights and freedoms.
- 5.2.2** If the LIA identifies a significant privacy impact Families First will consider whether they also need to conduct a Data Protection Impact Assessment (DPIA) (see section **9**).
- 5.2.3** Keep the LIA under review, and repeat it if circumstances change.
- 5.2.4** Include information about Families First legitimate interests in our relevant privacy notice(s).
- 6. Sensitive personal information**
- 6.1** Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.
- 6.2** It is unlikely that Families First will need to process sensitive personal information. We will only process sensitive personal information if:

6.2.1 We have a lawful basis for doing so as set out in section **5.1.1** above.

6.2.2 One of the special conditions for processing sensitive personal information applies, such as:

- The data subject has given explicit consent.
- The processing is necessary for the purposes of exercising the employment law rights or obligations of Families First or the data subject.
- The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
- The processing relates to personal data which is clearly made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for reasons of substantial public interest.

6.3 Before processing any sensitive personal information, staff must notify Families First Manager or Office Manager of the proposed processing; in order that they may assess whether the processing complies with the criteria noted above.

6.4 Sensitive personal information will not be processed until:

6.4.1 The assessment referred to in paragraph **6.3** has taken place.

6.4.2 The individual has been properly informed (by way of a Privacy Notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.5 Families First will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6.6 Where appropriate, Families First's Privacy Notices set out the types of sensitive personal information that Families First processes, what it is used for and the lawful basis for the processing.

6.7 In relation to sensitive personal information, during recruitment, Families First will comply with the procedures set out in section **6.8** and **6.9** below to make sure that it complies with the data protection principles set out in section **4** above.

6.8 During the recruitment process Families First will ensure that (except where the law permits otherwise):

6.8.1 During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, such as race or ethnicity, trade union membership or health.

6.8.2 If sensitive personal information is received from the applicant without being asked for it within their application form, CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted.

- 6.8.3** Should Families First collate equal opportunities information, it will be kept separate from the individual's application form and will not be seen by the person shortlisting, interviewing or making the recruitment decision.
- 6.8.4** Right to work checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages.
- 6.8.5** Families First will only ask health questions once an offer of employment has been made.

6.9 During employment Families First will process:

- 6.9.1** Health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits.
- 6.9.2** Sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised.
- 6.9.3** Trade union membership information for the purposes of staff administration and administering 'check off'.

7. Personal Information and third parties

7.1 Families First process personal data from third parties, these could include:

- Service users.
- Funders.
- Referring agencies.
- Medical professional.

7.2 Data will be processed for specific lawful purposes in accordance with the data protection principles and as set out in the relevant Privacy Notices as appended to this Policy.

8. Criminal records information

8.1 Where Families First is required to process criminal records information (PVG, personal disclosures or new information), it will be processed in accordance with the data protection principles.

9. Data Protection Impact Assessments (DPIA)

9.1 Where processing is likely to result in a high risk to an individual's data protection rights for example where Families First is planning to use a new form of technology), we will, before commencing the process, carry out a DPIA (appendix G) to assess:

- 9.1.1 Whether the processing is necessary and proportionate in relation to its purpose.
- 9.1.2 The risks to individuals.
- 9.1.3 What measures can be put in place to address those risks and protect personal information.

- 9.2 Before any new form of technology is introduced, the Manager will discuss with the (business support) team an appropriate way forward in order that a DPIA can be carried out.
- 9.3 During the course of any DPIA Families First will seek the advice of any other relevant stakeholders who could offer guidance to minimise the impact of any data breaches.

10. Data Protection Officer (DPO)

- 10.1 A data protection officer can be appointed voluntarily by an organisation, but is not always necessary.
- 10.2 There are certain situations prescribed by the GDPR where a DPO is required by law.
- 10.3 Guidance regarding this can be found on the [Information Commissioners website under Article 29 Working Party Guidance on Data Protection Officers](#).
- 10.4 Families First does not, at the time of writing this policy, need to appoint a Data Protection Officer as by law we do not fit the required criteria. Under the GDPR Families First must appoint a DPO if:
 - We are a public authority or body (except for courts acting in their judicial capacity).
 - Our core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking).
 - Our core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

11. Documentation and records

- 11.1 Families First will keep written records of activities which involve sensitive personal information, including:
 - 11.1.1 Families First referral, registration, review and ending forms.
 - 11.1.2 Minutes, notes and correspondence from 3rd parties pertaining to the wellbeing of a service user. All contained within the service users personal file.
 - 11.1.3 The purpose of the processing.
 - 11.1.4 A description of the categories of individuals and categories of personal data.
 - 11.1.5 Where possible, retention schedules.
 - 11.1.6 Where possible, a description of technical and organisational security measures.

- 11.2** Families First will document, or link to documentation, on:
- 11.2.1** Information required for privacy notices.
 - 11.2.2** Records of consent.
 - 11.2.3** Controller-processor contracts.
 - 11.2.4** The location of personal information.
 - 11.2.5** LIA.
 - 11.2.6** DPIA.
 - 11.2.7** Records of data breaches.
- 11.3** If Families First process sensitive personal information or criminal records information, they will keep written records of:
- 11.3.1** The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose.
 - 11.3.2** The lawful basis for processing.
 - 11.3.3** Whether we retain and erase the personal information in accordance with our Retention of Records policy and, if not, the reasons for not following our policy.
 - 11.3.4** Families First will conduct regular reviews of the personal information we process and update our documentation and policies accordingly.
- 11.4** Families First may document its processing activities in electronic or hard copy form so information can be easily updated in the event of change.

12. Privacy notices

- 12.1** Families First will issue Privacy Notices informing people about the personal data that we collect and hold on them and how they can expect their personal information to be used and for what purposes. This includes third parties where applicable.
- 12.2** Families First will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

13. Individual rights, Subject Access Requests (SAR)

- 13.1** Individuals have the following rights in relation to the personal information we hold on them:
- 13.1.1** To be informed about how, why and on what basis their information is being processed.
 - 13.1.2** To obtain confirmation that their information is being processed and that they can obtain access to it and certain other information, by making a [subject access request](#).
 - 13.1.3** To have data corrected if it is inaccurate or incomplete.

- 13.1.4** To have data erased if it is no longer necessary for the purpose for which it was originally processed, or if there are no overriding legitimate grounds for the processing, this is sometimes known as 'the right to be forgotten'.
- 13.1.5** To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they may not want the data to be erased), or where Families First no longer needs the personal information but require the data to establish, exercise or defend a legal claim.
- 13.1.6** To restrict the processing of personal information temporarily whilst Families First is verifying whether it is accurate.
- 13.1.7** If a data subject objects to the processing of personal data Families First reserve the right to decline a service or offer of employment.
- 13.2** Individuals can make a subject access request verbally or in writing.
- 13.3** Families First have created a form for people to use should they want to (appendix H). This form is not compulsory; staff may use this form when dealing with a telephone request or to attach an email request.
- 13.4** Families First will respond within 28 days to the request.
- 13.5** Families First will not charge a fee to deal with the request, unless:
- It is manifestly unfounded or excessive.
 - An individual requests further copies of their data following a request.
- 13.6** Subject access requests for children should be given the same amount of due consideration as an adult.
- 13.6.1** It is the child who has a right of access to the information Families First hold about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.
- 13.6.2** Families First need to consider if a child is too young to understand the implications of subject access rights as it is still the right of the child rather than of anyone else such as a parent or guardian.
- 13.6.3** Before responding to a subject access request for information held about a child Families First will consider whether the child is mature enough to understand their rights.
- 13.6.4** If we feel confident that the child can understand their rights, then we will respond directly to the child.
- 13.6.5** Families First will allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.
- 13.6.6** What is important to Families First is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.
- 13.6.7** When considering borderline cases Families First will take the following into consideration, along with any other information:
- The child's level of maturity and their ability to make decisions such as this.

- The nature of the personal data.
- Any court orders relating to parental access or responsibility that may apply.
- Any duty of confidence owed to the child or young person.
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

13.6.8 Families First may seek professional guidance, without disclosing personal information, from the [Scottish Child Law Centre](#) or the [Children and Young People's Commissioner Scotland](#) when supporting a child through a SAR.

13.7 If you wish to exercise any of the rights in this section, please contact Families First Manager or Office Manager.

14. Individual obligations

14.1 Individuals are responsible for helping Families First keep their personal information up to date. They should contact the Office Manager if the information they have provided to Families First changes, for example:

- Change of address.
- Change of bank details.
- Change of phone number.
- Change of emergency contact.

14.2 If staff have access to the personal information of other members of staff, volunteers, service users, customers or suppliers, partners or funders of Families First in the course of their employment, Families First expects the employee to help meet its data protection obligations to those individuals.

14.3 If staff or volunteers have access to personal information, they must:

14.3.1 Only access the personal information they have authority to access and only for authorised purposes.

14.3.2 Only allow other staff or volunteers to access personal information if they have appropriate authorisation.

14.3.3 Only allow individuals who are not staff or volunteers from Families First to access personal information if they have specific authority to do so from the Manager.

14.3.4 Keep personal information secure by complying with rules on access to premises, computer access, password protection and secure file storage

and destruction and other precautions set out in Families First's Confidentiality Policy.

- 14.3.5** Not remove personal information, or devices containing personal information (or which can be used to access it), from Families First's premises unless appropriate security measures are in place (such as pseudonymisation, encryption and/or password protection) to secure the information and/or the device.
 - 14.3.6** Not store personal information on local drives or on personal devices that are used for work purposes; staff must comply with Families First's ICT policy.
- 14.4** Individuals should contact Families First Manager if they are concerned or suspect that one of the following has taken place (or is taking place or is likely to take place):
- 14.4.1** Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph **6.2.2** being met.
 - 14.4.2** Any data breach as set out in paragraph **17.1** below.
 - 14.4.3** Access to personal information without the proper authorisation.
 - 14.4.4** Personal information not kept or deleted securely.
 - 14.4.5** Removal of personal information, or devices containing personal information (or which can be used to access it), from Families First's premises without appropriate security measures being in place.
 - 14.4.6** Any other breach of this policy or of any of the data protection principles set out in paragraph **4.1** above.

15. Information security

- 15.1** Families First will use appropriate technical and organisational measures in accordance with its policies on information security to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
- 15.1.1** Making sure that, where possible, personal information is pseudonymised or encrypted.
 - 15.1.2** Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
 - 15.1.3** Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner.
 - 15.1.4** A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 15.2** Where Families First uses external organisations to process personal information, on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must stipulate that:

- 15.2.1** The external organisation may act only on the written instructions of Families First.
 - 15.2.2** Those processing the data are subject to a duty of confidence.
 - 15.2.3** Appropriate measures are taken to ensure the security of processing.
 - 15.2.4** Sub-contractors are only engaged with the prior consent of Families First and under a written contract.
 - 15.2.5** The external organisation will assist Families First in providing subject access and allowing individuals to exercise their rights in relation to data protection.
 - 15.2.6** The external organisation will assist Families First in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments.
 - 15.2.7** The external organisation will delete or return all personal information to Families First as requested at the end of the contract.
 - 15.2.8** The external organisation will submit to audits and inspections, provide Families First with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Families First immediately if it is asked to do something infringing data protection law.
- 15.3** Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms from the Office Manager.

16. Storage and retention of personal information

- 16.1** Personal information (and sensitive personal information) will be kept securely and for no longer than necessary in accordance with Families First's Retention of Records Policy.
- 16.2** The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.
- 16.3** Staff should follow Families First's Retention of Records Policy which sets out the relevant retention periods for a variety of data. Where there is any uncertainty, staff should consult Families First Manager.
- 16.4** Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed by shredding.

17. Data breaches

- 17.1** A data breach may take many different forms, for example:
 - 17.1.1** Loss or theft of data or equipment on which personal information is stored.
 - 17.1.2** Unauthorised access to or use of personal information either by a member of staff or third party.
 - 17.1.3** Loss of data resulting from an equipment or systems (including hardware and software) failure.
 - 17.1.4** Human error, such as accidental deletion or alteration of data.
 - 17.1.5** Unforeseen circumstances, such as a fire or flood.

17.1.6 Deliberate attacks on IT systems, such as hacking, viruses or phishing scams.

17.1.7 Blagging' or social engineering offences, where information is obtained by deceiving the organisation which holds it.

17.2 In the event of a data breach Families First will:

17.2.1 Make the required report, if necessary, to the Information Commissioner's Office without undue delay and, where possible, within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals.

17.2.2 Notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

17.3 Information regarding the breach may be held at more than one location depending on the nature of the breach such as Families First offices, third-party agencies and representatives of Families First (appendix J).

17.4 Dependant on the severity of the breach Families First Manager will decide the best course of action to take, involving the service user, and or their carers if there is a capacity issue.

18. Training

18.1 Families First will ensure that staff are adequately trained regarding their data protection responsibilities.

18.2 Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

19. Consequences of failing to comply

19.1 Failure to comply with the policy can result in:

19.1.1 Putting individuals at risk.

19.1.2 Carries the risk of civil and criminal proceedings for the individual and Families First.

19.1.3 May, in some circumstances result in a criminal offence by the individual.

19.2 Due to the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct.

19.3 If a non-employee breaches this policy, they may have their contract or, in the case of volunteers their volunteer agreement, terminated with immediate effect.

19.4 If you have any questions or concerns about anything in this policy, do not hesitate to contact:

- Families First Manager, Morag Coleman, on:

- 01334 208086
 - Email manager@familiesfirststandrews.org.uk
 - Facebook messenger <https://www.facebook.com/> and search for Morag Coleman.
- or, The Information Commissioner's Office (ICO) at:

The Information Commissioner's Office
45 Melville Street
Edinburgh
EH3 7HL
 - Telephone: 0303 123 1115
 - Email: Scotland@ico.org.uk
- 20.** I have read and understood this policy and agree to abide by its terms.

Signed:

Date:

Appendix A

Privacy notice staff

I attach an Employee Data Protection Privacy Notice which you should read carefully and keep in a safe place as it contains important information about:

- Which information we collect and how and why we do so.
- Who collects personal information about you.
- How we use the information and who we may share it with.
- Any monitoring we may undertake.
- Where we may hold your personal information.
- How long we keep your information.
- Your rights to correct and access your information and to ask for it to be erased.
- Details of where you can find further information about some of the matters listed above.
- How to complain if we get things wrong and cannot resolve them for you.

We are sending you this notice to make sure we comply with current legislation governing data protection. We are not making any significant changes to the way in which we administer your information or the reasons for why we do so. We are being more open and transparent about the information we process about you.

Appendix B

Privacy notice volunteers

Please note a record of all your personal information will be kept in a secure file, on our computer system, and in locked filing cabinets, at our Families First office in St Andrews.

Access to these records is restricted to Families First staff and will only be shared with a third party if we have any concerns for your, a child or an adult's wellbeing; in compliance with Families First confidentiality, GDPR and child and adult protection policies.

The information you provide is used exclusively for your volunteering role.

Appendix C

Privacy Notice Adult Service Users

Personal data supplied on this form will be held as a paper copy (in a locked filing cabinet) and on computer (password protected) and used in accordance with GDPR 2018.

All data and information received and held by Families First is used solely for the purposes of:

- Offering meaningful services.
- Collating anonymised statistics for reporting to funders about the work we do.
- Collating anonymised statistics to apply for funding.
- Protecting vulnerable children and adults.

Families First also have a policy (Retention and Disposal of Confidential Records) which states how long we keep personal information for.

Under normal circumstances, unless there has been an incident of concern, we keep all personal information on service users for a year after leaving service. We do this in case any immediate queries are raised, or the service user should return into service.

After a year, we keep a factual record of name, dates in service, services used, reason for being in service and names of staff and volunteers who worked with the service user. We keep this information in case it is required, in the future, for child and adult protection purposes.

Privacy Notice Child Service Users

Please provide as much information as possible to help us make an informed assessment as to the person's suitability for Families First services.

All data and information received and held by Families First, in line with the General Data Protection Regulation (GDPR) 2018, is used solely for the purposes of:

- Offering meaningful services.
- Collating anonymised statistics for reporting to funders about the work we do.
- Collating anonymised statistics to apply for funding.
- Protecting vulnerable children and adults.

Personal data supplied on this form will be held as a paper copy (in a locked filing cabinet) and on computer (password protected) and used in accordance with GDPR 2018.

Families First also have a policy (Retention and Disposal of Confidential Records) which states how long we keep personal information for.

Under normal circumstances, unless there has been an incident of concern, we keep all personal information on service users for a year after leaving service. We do this in case any immediate queries are raised, or the service user should return into service.

After a year, we keep a factual record of name, dates in service, services used, reason for being in service and names of staff and volunteers who worked with the service user. We keep this information in case it is required, in the future, for child and adult protection purposes.

Appendix D

Privacy notice website

Families First is committed to respecting the privacy rights of all visitors to our website.

We comply with data protection laws at all times and have set out this Privacy Notice to explain what personal data we collect, why we collect it, how we protect it, and to explain your rights.

We collect the following data about you when you complete forms on our website:

- Your name, e-mail address, contact details and communication preferences.

Our website is not intended for use by children and as such we do not knowingly collect any data relating to children.

We are committed to keeping your data secure. We use encryption for web traffic to and from our website and we store any data provided through our website in secure computer systems that only authorised staff and volunteers have access to.

We use your data for three reasons:

- To provide information, support and services.
- To manage customer service interactions.
- To analyse anonymous data to enhance our business activities and reach.

Appendix E

Privacy notice Facebook

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

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

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

Reviewed by Manager and Office manager 20 January 2020

Appendix F
Families First Legitimate Interests' Assessment (LIA) form

All data and information received and held by Families First, in line with the General Data Protection Regulation (GDPR) 2018, is used solely for the purposes of:

- Offering meaningful services.
- Collating anonymised statistics for reporting to funders about the work we do.
- Collating anonymised statistics to apply for funding.
- Protecting vulnerable children and adults.

Personal data supplied on this form will be held as a paper copy (in a locked filing cabinet) and on computer (password protected) and used in accordance with GDPR 2018. The information provided on this form will help Families First deal with the assessment outlined below.

Under normal circumstances, unless there has been an incident of concern, we keep all personal information on service users for a year after leaving service. We do this in case any immediate queries are raised, or the service user should return into service.

After that year we keep a factual record of name, dates in service, services used, reason for being in service and names of staff and volunteers who worked with the service user. We keep this information in case it is required, in the future, for child and adult protection purposes.

| | |
|---|--|
| Name of data subject | |
| Date of LIA | |
| What is the reason for processing the data? | |
| Why is the processing necessary? | |
| Is there a legal basis for processing this data? <ul style="list-style-type: none"> • <i>The data subject has given explicit consent.</i> • <i>The processing is necessary for the purposes of exercising the employment law rights or obligations of Families First or the data subject.</i> • <i>The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving</i> | |

| | |
|---|--|
| <p><i>consent.</i></p> <ul style="list-style-type: none"> • <i>Processing relates to personal data which is clearly made public by the data subject.</i> • <i>The processing is necessary for the establishment, exercise or defence of legal claims.</i> • <i>The processing is necessary for reasons of substantial public interest.</i> | |
| <p>How will this affect the individual's interests, rights and freedoms?</p> | |
| <p>Have you discussed this with Families First Manager or Office Manager?</p> | |
| <p>Has the data subject consented to the processing of their data?</p> | |
| <p>How long must FF keep this assessment? Please explain why</p> | |
| <p>Data subject print name:</p> | |
| <p>Data subject sign:</p> | |
| <p>Data subject date:</p> | |
| <p>Staff member print name:</p> | |
| <p>Staff member sign:</p> | |
| <p>Staff member date:</p> | |

Appendix G
Data Protection Impact Assessments (DPIA)

| | |
|---|--|
| What is the activity that needs a DPIA? | |
| Date of DPIA: | |
| Will the processing of data pose a high risk to an individual's data protection rights? | |
| Is the processing necessary and proportionate in relation to its purpose? | |
| What are the risks to FF people? | |
| What can we do to minimise those risks and protect personal information? | |
| Have you discussed this with Families First Manager or Office Manager? | |
| How long must FF keep this assessment? Please explain why. | |
| Staff member print name: | |
| Staff member sign: | |
| Staff member date: | |

Appendix H

Subject Access Request (SAR) form

All data and information received and held by Families First, in line with the General Data Protection Regulation (GDPR) 2018, is used solely for the purposes of:

- Offering meaningful services.
- Collating anonymised statistics for reporting to funders about the work we do.
- Collating anonymised statistics to apply for funding.
- Protecting vulnerable children and adults.

Personal data supplied on this form will be held as a paper copy (in a locked filing cabinet) and on computer (password protected) and used in accordance with GDPR 2018. The information provided on this form will help Families First deal with the request outlined below.

Under normal circumstances, unless there has been an incident of concern, we keep all personal information on service users for a year after leaving service. We do this in case any immediate queries are raised, or the service user should return into service.

After that year we keep a factual record of name, dates in service, services used, reason for being in service and names of staff and volunteers who worked with the service user. We keep this information in case it is required, in the future, for child and adult protection purposes.

| | |
|---|--|
| Name of person asking for the information? | |
| Date of request: | |
| What information would you like? | |
| Why would you like this information? | |
| Are there specific dates that would help Families First find the information you require? | |
| Any other useful information? | |
| Sign: | |
| Date: | |

Appendix I
Families First response form for dealing with a subject access request

All data and information received and held by Families First, in line with the General Data Protection Regulation (GDPR) 2018, is used solely for the purposes of:

- Offering meaningful services.
- Collating anonymised statistics for reporting to funders about the work we do.
- Collating anonymised statistics to apply for funding.
- Protecting vulnerable children and adults.

Personal data supplied on this form will be held as a paper copy (in a locked filing cabinet) and on computer (password protected) and used in accordance with GDPR 2018. The information provided on this form will help Families First deal with the request outlined below.

Under normal circumstances, unless there has been an incident of concern, we keep all personal information on service users for a year after leaving service. We do this in case any immediate queries are raised, or the service user should return into service.

After that year we keep a factual record of name, dates in service, services used, reason for being in service and names of staff and volunteers who worked with the service user. We keep this information in case it is required, in the future, for child and adult protection purposes.

| | |
|--|--|
| Name of person asking for the information? | |
| Date of request: | |
| What information would they like? | |
| Why do they want this information? | |
| Are there specific dates that would help Families First find the information? | |
| Any other useful information? | |
| What did Families First do about this request? | |
| Did Families First need to involve 3 rd parties? If so, please state why. | |

| | |
|-------------|--|
| Print name: | |
| Sign: | |
| Date: | |

Appendix J
Families First Data Breach form

All data and information received and held by Families First, in line with the General Data Protection Regulation (GDPR) 2018, is used solely for the purposes of:

- Offering meaningful services.
- Collating anonymised statistics for reporting to funders about the work we do.
- Collating anonymised statistics to apply for funding.
- Protecting vulnerable children and adults.

Personal data supplied on this form will be held as a paper copy (in a locked filing cabinet) and on computer (password protected) and used in accordance with GDPR 2018. The information provided on this form will help Families First deal with the data breach outlined below.

Under normal circumstances, unless there has been an incident of concern, we keep all personal information on service users for a year after leaving service. We do this in case any immediate queries are raised, or the service user should return into service.

After that year we keep a factual record of name, dates in service, services used, reason for being in service and names of staff and volunteers who worked with the service user. We keep this information in case it is required, in the future, for child and adult protection purposes.

| | |
|---|--|
| Name of person notifying the breach? | |
| Date of notification: | |
| What do they believe has happened? | |
| When did the breach happen? | |
| When was the breach discovered? | |
| How did it happen? | |
| Did FF have measures in place that could have stopped the breach? | |
| How many people have been affected by the breach? | |
| What is the potential detriment to people? | |

| | |
|--|--|
| Have people been notified about the breach? | |
| What measures have been taken to help people affected by the breach? | |
| Do we need to notify the ICO? | |
| Have the ICO been notified (within 72 hrs)? | |
| How can FF stop similar breaches in the future? | |
| Print name: | |
| Sign: | |
| Date: | |