Family Futures General Data Protection Regulation (GDPR) policy

Policy information	
Organisation	Family Futures CIC
Scope of policy	This Policy forms part of a suite of policies and procedures that supports our information governance framework. Other related policies include: • Confidentiality Policy • Privacy Policy • Information Security Policy • Safeguarding Children & Young People policy • Working at Home Policy • Freedom of Information policy • Records Management policy • Reporting Data Protection and Information Security Incidents This policy applies to all personal data handled by Family Futures, including data held in paper files and data held electronically. As long as the processing of data is carried out on Family Futures' behalf it applies to any individual who processes that data (including volunteers) and applies regardless of where the data is held, (for example, it covers data held on mobile devices such as electronic notebooks, laptops or mobile phones) and regardless of who owns the PC/device on which it is stored. The 'processing' of data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining, recording, keeping or using it in any way; sharing or disclosing it; erasing and destroying it.
Policy operational date	25th May 2018
Policy prepared by	Deborah Prosper, Agency Administrator & Data Protection Lead
Date approved by Services Manager' Team	
Policy review date	July/August 2018 - to ensure that once the bill becomes law, FF is compliant

	with all requirements then every two years thereafter - May 2020

Introduction

Purpose of policy

Family Futures is committed to being transparent about how it collects and uses the personal data of its workforce, clients and any other individuals, and to meeting its data protection obligations.

This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

Brief introduction to Data Protection legislation

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. It is a new legal framework for data protection and is intended to strengthen and unify data protection for individuals within the European Union (EU). The GDPR replaces the 1998 Data Protection Act and is supported by the UK's Data Protection Act 2018, which became law on the same date. In addition, the Privacy & Electronic Communications Regulation 2003 (and a new ePrivacy Regulation which will eventually replace it) makes additional rules about direct marketing by phone, email or text.

Key points of the legislation are:

- The Regulations apply to '**personal data**', which includes both written and computerised information about individuals who can be identified *in any way*, even if their name is not known.
- Types of personal data whose misuse could have the greatest impact on Data Subjects ('special category' data) are more tightly controlled.
- Responsibility for compliance rests with Family Futures as an organisation.
- Any use of personal data must have a recognised '**legal basis**'.
- Any use of personal data must comply with the '**Data Protection Principles**'.
- The Regulations grant a number of rights to individuals, including the right to know what information an organisation holds about them.

Responsibilities

All Family Futures paid staff (and volunteers) are required to follow this Data Protection Policy at all times. They are also required to be familiar with the privacy notice(s) relevant to their area of work, and to ensure that the undertakings given to Data Subjects are complied with.

The Services' Managers Team has overall responsibility for data protection within Family Futures but each individual processing data is expected to understand how data protection applies to their own area of work.

Policy statement & Objectives

Family Futures understands the importance of ensuring that personal data, including special category data is always treated lawfully and appropriately and the rights of the individual are upheld. Family Futures collects, holds, uses and shares personally identifiable information about its staff and clients for the purposes of delivering services, carrying out our statutory obligations and meeting the needs of the individuals that we deal with.

It is Family Futures' policy to comply with both the spirit and letter of the law contained in the GDPR and we will ensure that:

- Any personal data will be collected, used and held, lawfully and appropriately.
- Regular data sharing with external partners and other relevant agencies will be subject to information sharing agreements.
- External agencies contracted to undertake any data processing on behalf of Family Futures will be required to demonstrate compliance with the Data Protection Act and satisfy Family Futures that they have the necessary technical and organisational measures in place to protect personal data, as well as meeting other contractual obligations required under GDPR.
- There are policies and procedures in place which are regularly reviewed and updated to ensure staff understand their responsibilities towards protecting personal data.
- Training needs are identified and provided to ensure that those handling personal data are trained appropriately.
- There is an appointed member of staff within the organisation who has specific responsibility and knowledge about data protection compliance covering all aspects within the scope of this policy and who is a point of contact for all queries.
- There are a number of employees throughout the organisation who have specific responsibilities for data protection.
- Data Subjects' rights can be fully exercised.
- Subject Access Requests are dealt with promptly and courteously.
- Any new projects being implemented that involve personal data will undergo a privacy impact assessment, and will incorporate data protection provision by default and by design.

We will regularly review and update this policy, procedures and guidance for Family Futures' employees and volunteers.

Legal basis

Family Futures (FF) recognises that no processing of personal data may take place unless it is within the scope of one of the six legal bases set out in GDPR. Family Futures therefore

establishes a sound legal basis before embarking on any processing of personal data and aims to select the most appropriate basis in each case.

Under the GDPR, the possible legal bases for processing personal data are:

(a) Consent: the member of staff/parent/child/young person has given clear, informed and unambiguous consent for FF to process their personal data for a specific purpose.

(b) Contractual necessity: the processing is necessary for a member of staff's employment contract or in order for FF to fulfil its contract with a Local Authority and/ or family.

(c) Legal obligation: the processing is necessary for FF to comply with the law (not including contractual obligations).

(d) The processing is necessary for protecting the vital interests of a data subject or another person. This would most often be in safeguarding instances, and in emergencies.

(e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(f) Processing that FF has determined to be necessary in its legitimate interests, or the legitimate interests of a third party, provided that no Data Subject's rights, freedoms or legitimate interests should take precedence.

Where Family Futures considers 'legitimate interests' to be the most appropriate legal basis, the reasoning for this is documented in a Legitimate Interests Assessment.

The legal bases for typical processing of personal data by Family Futures are described in the relevant privacy notices.

Where anyone acting on behalf of Family Futures is unsure of the appropriate legal basis they should consult the Data Protection Lead before beginning any processing of personal data.

Data Protection Principles

Family Futures is required to process personal data in accordance with the six data protection principles:

a) Personal data must be processed lawfully, fairly and in a transparent manner.
b) Personal data must be collected only for specified, explicit and legitimate purposes.
c) Personal data must be adequate, relevant and limited to what is necessary for the purposes for which it is to be processed.

d) Personal data must be accurate and where necessary up to date. FF must takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
e) Personal data must be retained no longer than necessary.
f) FF must adopt appropriate measures to ensure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

In relation to the requirement for transparency set out in the first Data Protection Principle, Family Futures tells individuals through 'privacy notices' the reasons for processing their personal data, how it uses such data and the legal basis for processing. Full privacy notices can be found at the end of this document. Key information is provided prominently whenever data is collected from Data Subjects. FF will not process personal data of individuals in ways that are outside the reasonable expectations of its Data Subjects.

'Special category' data

Additional restrictions apply to certain types of personal data which would pose a bigger risk to Data Subjects if it were misused. Often the explicit consent of the Data Subject is required. This 'special category' data includes the Data Subject's:

- Racial or ethnic origins
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data
- Biometric data that can be used to identify them
- Health
- Sex life or sexual orientation

Similar restrictions also apply to the use of data about an individual's criminal record.

Information on how special category data may be used at Family Futures can be found in the detailed sections below.

Responsibilities

Services' Managers Team

The **Services' Managers Team (SMT)** is ultimately responsible for ensuring that Family Futures CIC meets its legal obligations.

Data Protection Lead

Family Futures has appointed Deborah Prosper, Agency Administrator as the person with responsibility for data protection compliance within the organisation. She can be contacted

at deborahp@familyfutures.co.uk. Questions about this policy, or requests for further information, should be directed to her.

The Data Protection Lead, Deborah Prosper, is responsible for:

- Keeping the SMT updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with Subject Access Requests' and other non-routine requests by individuals to exercise any of their rights under GDPR.
- Checking and approving any contracts or agreements with third parties that may be acting as a Data Processor or Joint Data Controller.

The Data Protection Lead will work in consultation with Data Protection expert Paul Ticher who will provide GDPR support. He can be reached at paul@paulticher.com but requests for support should normally be passed on via the Data Protection Lead.

The Agency Administrator, Deborah Prosper in liaison with Family Futures' IT provider Coop Sys, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating the security provisions offered by any third-party services the company is considering using to store or process data. For instance, cloud computing services.

Specific other staff

Marketing Communications Specialist, Rosemary Watson is responsible for:

- Approving any data protection statements attached to marketing communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets e.g. newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Team/Department managers

Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

All staff & volunteers

Staff and volunteers may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract or volunteer period. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and clients.

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 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);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes unless this has been specifically authorised by the Data Protection Lead.

Further details about Family Futures' security procedures can be found in our IT/Network security policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Individuals who cause or become aware of a data breach, a possible breach or a "near miss" are required to report this immediately to the Data Protection Lead so that remedial action can be taken promptly. Failure to report a breach promptly may be treated as gross misconduct.

Staff training & acceptance of responsibilities

Induction: Family Futures will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Continuing training: Individuals whose roles require regular access to personal data, 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. There will also be opportunities to regularly offer staff training on practical data protection issues such as clearing out old information, keeping their access passwords secure etc. during team meetings and supervision sessions.

Family Futures will also provide annual Data Protection briefings/training provided by our Data Protection consultant, Paul Ticher.

Procedure for staff signifying acceptance of policy: Some thought should be given as to what staff are going to be asked to sign up to. This policy? Or the procedures in their own team or department?

Security

Scope

Keeping personal data properly secure is key to complying with GDPR and Family Futures takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are – in particular – obliged to implement appropriate technical and organisational measures to ensure the security of data.

Keeping data secure

Managers must be sure that adequate measures are taken to ensure the security of files. All staff are responsible for ensuring that if they keep any personal data, it is kept securely and is not disclosed (either orally, in writing or accidentally) to any unauthorised third party.

The most common causes of data loss or leakage and breaches of the Act can be avoided by following the guidance below:

- Confidential paper files should be kept in locked cabinets or locked offices when not being used, and should be stored securely at the end of the day – not left on desks.
- Offices should be locked when left unattended (during meetings and lunch breaks).
- Users must ensure that they always log off from the computer when away from it.
- Password protection should be used for any electronic files/documents containing confidential personal data.
- Particular care must be taken when transferring personal data onto a memory stick, laptop or any other mobile device – using password protection and encryption where appropriate.

- If there is ever a need to send confidential personal data by email egress should be used where appropriate or else the confidential material should be attached in a password-protected document (and the password MUST NOT be conveyed to the recipient by email – it should be given verbally or by text).
- Passwords must use a minimum of 8 or more characters, including lowercase and uppercase alphabetic characters, numbers and symbols.
- Additional provisions in Family Futures' IT/Network Security Policy must be adhered to.
- Copies of confidential personal data should not be made unless it is strictly necessary.

Restricting access to personal data

Managers must ensure that access to data is only granted to staff who require it for legitimate purposes.

All staff must ensure that they disclose personal data to third parties only where this has been authorised, and falls within the reasonable expectations of the Data Subjects.

Where personal data needs to be shared routinely with a third party for business purposes a data sharing agreement must be entered into with them, after consultation with the Data Protection Lead.

All staff should in addition be familiar with the relevant sections of the company's VAA Manual that apply to their area of work.

Business continuity

Backups are carried out daily and the tapes are held securely in a fireproof safe. The weekly backup tape is taken off site, in control of the Agency Administrator.

For full details of the organisation's business continuity plan, please refer to the Disaster Recovery Policy.

Disposal of information

When personal data is no longer required it must be disposed of carefully.

Shred paper files or dispose of them securely using the confidential waste bin.

If you store personal data on your own device you must securely erase all personal data on it before disposing of it.

Transparency

Family Futures recognises its obligation to be transparent about its data processing activities. Privacy Notices are in place – and regularly reviewed – for different categories of Data Subject, in particular for clients and for employees and volunteers.

These Privacy Notices must be made available to Data Subjects at appropriate times, especially when individuals first come into contact with Family Futures.

Further information about the processing of staff's data can be found in our *Privacy Notice for Staff* in Appendix 1 (and in the Staff Handbook and FF CIC Policies & Procedures Manual for all Staff 2018) and for parents and carers in *Privacy Notice for Parents and Carers* in Appendix 2 and for children in *Privacy Notice for Children* in Appendix 3.

In addition, whenever data is collected from individuals, relevant summaries of key information from the applicable privacy notice must be communicated directly to the individual along with the request for information. Standard wording is provided by Family Futures for use in typical situations where data is sought on forms (paper or online) or verbally.

Where Family Futures bases its processing on consent this is obtained routinely (e.g. when a parent completes a parent contract, when a job applicant submits an application or when a new member of staff signs a contract of employment). If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

Records with respect to services

Each child and their family where work has been commissioned has an electronic case file which is password-protected. There is also a paper file which holds:

- Basic biographical information of all family members
- Contracts
- Notes of sessions
- Assessments carried out and assessment reports
- Information provided by the commissioning agency and the family
- Copies of all correspondence
- Outcome monitoring reports from the six-monthly case review.

All paper files are updated by administrative staff, the responsibility for which rests with the Therapy Services Lead Coordinator in the first instance. The keyworker for each family is responsible for ensuring that all relevant information is updated on the file.

These files are kept in locked cabinets.

All records are kept in compliance with Standard 27 in the Department for Education's Adoption: National minimum standards 2014.

We are required by law to share or make available some of the personal data we collect and hold. This information may be shared with local authorities or social services for the purposes of the provision of social care or treatment; to safeguard public funds and for the prevention and detection of fraud, and for the prevention and detection of crime. For more details on this please read our Privacy Notice.

Policy on Case Recording

Any record kept regarding the client is kept at all times under the highest levels of confidentiality.

Case records would normally be typed and are the responsibility of the keyworker for the case, who would normally be operating at a senior practitioner level. Assessment reports, network reports and any other case summary will be dated and signed by the keyworker and a Service Manager.

Clients have the right to make a subject access request at any time. Third party information may be removed where disclosure would infringe the third party's confidentiality.

To ensure the safety and confidentiality of paper records, they are kept in locked filing cabinets when not in active use.

The server is stored in a locked room at night.

Video footage of client sessions is filmed only with their consent and is kept in a locked cupboard. Once no longer required, these tapes are wiped.

All staff are made aware of these procedures as part of their induction programme.

To ensure the safety of client records, a highly sophisticated intruder alarm system with direct links to a key holding company is in operation.

Hand written records are clearly written and legible.

Any written/typed information in session notes, reports or summaries are clearly expressed in a non-stigmatizing way and differentiate clearly between fact and opinion.

See VAA Manual 'Presentation of Family Futures Documents'.

Adoption Agencies

Family Futures gives information from its case files promptly to other adoption agencies and local authorities to effect the placement of a child.

Family Futures' procedures take account of Data Protection legislation and the Human Rights Act and cover:

- Authorising access to adoption case records and their indexes and disclosure of adoption information
- When to make records or information available under the Adoption Agencies Regulations 1983 and 2005
- How to deal with requests for access or disclosure and who can authorise them
- The requirement for a written confidentiality agreement before disclosure (this does not cover the child or adopter but covers anyone else in or outside the agency, including the adoption panel).

Electronic/Paper Documents Taken From Family Futures' Office for Home Use

Any paper document relating to a case, if taken from the Family Future' offices for home use, must be kept in a locked cabinet and must be transported in a locked case. Original documents should not be taken, but photocopied.

When working out of the office on a computer all electronic documents should be kept on an encrypted memory stick which is provided by Family Futures for all staff members.

Case files retention periods

Some records, such as those relating to child protection, fostering and adoption are subject to statutory requirements and have a specific retention period:

An "adoption agency must keep information in relation to a person's adoption for at least 100 years from the date of the adoption order (Section 56, Adoption and Children Act 2002 and Reg. 6 Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005)". This includes all assessment and treatment, and adoption cases.

Looked After Children records are kept for 75 years

The records on the assessment process to check the suitability of prospective adoptive parents that subsequently led to a placement are retained for 100 years from the date of adoption

Adopters where their application is refused or not proceeded with is kept for 10 years

Records of Consultations where they have not proceeded into assessment, are kept until the child reaches 18 years old or when the child reaches 24 years if they consented to the service

Information gathered in the process of an Initial Enquiry (that did not progress to assessment) are destroyed 1 year after closure

Complaints/Management Inquiries are retained for 6 years

Staff records – 25 years after their period of employment ended

Information about financial support is destroyed 6 years after the end of the financial year.

Research – Special considerations

Before commencing any research which will involve obtaining or using personal data, the researcher (member of staff) and their academic supervisor or Manager must give proper consideration to this policy and the guidance contained in within it and how these will be properly complied with.

In particular, they will need to consider the type of personal data which may be collated, how consent is to be recorded, the extent to which such data may legitimately be required for the academic objective, how the data will be securely stored, (particularly if the data is what might be considered to be security-sensitive) and the duration for which it will be retained.

Personal data obtained or used for research should be limited to the minimum amount of data which is reasonably required to achieve the desired academic objectives and wherever possible any such personal data should be made anonymous so that the data subjects cannot be identified.

Administrative Records

Family Futures keeps separate staff employment records. This system is managed by the Agency Administrator.

Entries on the record sheets are legible and factual, signed and dated. These records are kept in a locked filing cabinet. There is a system for keeping records of all complaints and allegations.

For concerns about any matter related to the safe keeping of records, staff should see the Grievance Policy and Whistle Blowing Policy in this Handbook.

Personnel Files of Members of Staff

Copies of the following are included in personnel files:

- Job descriptions and person specifications
- Application form & CV
- Copies of the employee's proof of right to work in the UK documentation
- References
- DBS checks (generally for six months, then a summary record)
- ID and professional membership registration details
- Appraisal and supervision notes
- Professional insurance cover if applicable
- Qualification certificates
- Training

- Holiday and sick leave record
- Any other matters related to staff employment.

Family Futures will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Staff records will be kept for 25 years from the date of the last entry in line with The Voluntary Adoption Agencies and Adoption Agencies (Miscellaneous Amendments) Regulations 2003.

Special category and criminal records data about a client or staff member will only be held without their express permission where it is necessary for compliance with our legal obligations (e.g. health and safety), to protect the individual's vital interests, or in a very limited range of other circumstances. Such information may also be retained as long as necessary for defending a complaint of unlawful discrimination or as a means of monitoring, promoting or maintaining our Equal Opportunities Policy.

The organisation keeps a record of its processing activities in respect of HR-related personal data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Managers' responsibilities

Managers must undertake a regular data cleanse of files to ensure that the data they contain is:

- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary.

Managers must be sure that adequate measures are taken to ensure the security of files:

- Whenever possible, store/save personal data on a Computing Services server.
- Never store personal data, especially sensitive personal data, on a mobile device or home computer unless it is strictly necessary and the device has been encrypted where appropriate.
- Don't store or transfer personal data where it could be lost or exposed (on unencrypted USB drives, mobile devices and laptops).

Managers should ensure their staff understand their rights and responsibilities under the GDPR.

In order to allow reasonable freedom of access to personal data managers are required to ensure their housekeeping is undertaken on a regular basis to ensure that through a wish to be open Family Futures is not compromised under the Act.

Retention periods

The GDPR states that data should not be kept for longer than is necessary for the purposes for which it is processed. Therefore, Family Futures sets out the following guidelines for retaining data. These guidelines relate to all those at the organisation who may hold information about paid staff or volunteers.

Application forms and interview notes (for unsuccessful candidates):

6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the personnel file in any event.)

Assessments under health and safety regulations and records of consultations with safety representatives and committees: – Permanently

DBS Checks: Once a recruitment (or other relevant) decision has been made, disclosure information is generally kept for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep disclosure information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding safe storage and strictly controlled access will prevail.

Once the retention period has elapsed, we may keep a record of the date of issue of a disclosure, the name of the subject, the type of disclosure requested, the position for which the disclosure was requested, the unique reference number of the disclosure and the details of the recruitment decision taken. All other disclosure information is immediately destroyed by secure means.

Parental Leave - 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance

Personnel files and training records (including disciplinary records and working time records) - 6 years after employment ceases for administrative staff and 25 years for therapy staff.

Senior Management records (that is, those on a senior management team or their equivalents) – Permanently for historical purposes

Statutory Sick Pay records, calculations, certificates, self-certificates - Although there is no longer a specific statutory retention period, employers still have to keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the

end of the period of sick leave in case of a disability discrimination claim. However if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.

It is important to remember that computer records as well as manual files are included in this policy.

Subject access and disclosure of data

Under GDPR, employees, volunteers and clients can, as "data subjects", make data subject access requests (SARs) in relation to information that is held about them.

Responsibility

The Data Protection Lead is responsible for processing SARs.

Procedure for making a Subject Access Request: Employees & volunteers

To gain access to information in your personnel file, you should submit a Subject Access Request in writing to the Agency Administrator. You are entitled to receive a copy of all the information held by Family Futures (with limited exceptions where this would infringe the confidentiality of someone else). However, if there is a specific piece of information or type of information that you wish to see, please say so, as this will speed up the response.

Under the law, information must be supplied within 30 days of the written request being received.

Access to references received will be provided as long as the provider of the reference has not specifically requested that Family Futures should not do so, and there is no other substantial reason for Family Futures to do otherwise.

Procedure for making a Subject Access Request or to exercise other Data Protection rights: Clients

Any member of staff receiving a request from a client for access to their data must pass this without delay to the Data Protection Lead, so that it can be responded to appropriately. Staff should **not** disclose data, either to the client or to a third party, without consulting the Data Protection Lead, other than as part of a routine data sharing arrangement.

To ensure that the request is processed quickly, clients should be encouraged to complete a Subject Access Request form, which can be downloaded from [our website]. This should be returned, with photocopies of suitable personal identification and proof of address (e.g. driving licence or passport) to the Data Protection Lead, either by email or by post.

Email the information to: deborahp@familyfutures.co.uk or if by post:

Data Protection Lead,
Family Futures CIC,
3 & 4 Floral Place,
7 – 9 Northampton Grove,
Islington,
London
N1 2PL.

Clients should be asked to be as specific as possible when outlining what data they want to see as this can help Family Futures locate and gather it. They may, within reason, request one copy of any or all of the information to which they seek access. A record will be made of any copies requested and provided, including date and place, together with the name of the person providing them. Clients will not normally be given a complete copy of a whole file as Subject access provides a right to have a copy of the information contained in personal data, rather than a right to all the documents that include that information.

If the request is made electronically, we will endeavour to provide the information in a commonly used electronic format. Some files may be too large to transmit electronically and we may have to supply it in CD format. The normal provision is for the required information to be provided "in permanent form". Alternatively, access to the information could be in the presence of a nominated person. The sole purpose of this is to ensure that no material is inappropriately removed or destroyed, and to prevent any such allegations at a later date.

Clients should be made aware that information may be excluded from access if it would infringe the confidentiality of another individual.

Requests for information about children

Under GDPR children merit specific protection with regard to their personal data and have the same rights as adults over their personal data, including the rights to access their personal data; (as well as to request rectification; object to processing and have their personal data erased). Even if a child is too young to understand the implications of subject access rights, data about them is regarded as their personal data and does not belong, for example, to a parent or guardian. Therefore, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised on their behalf by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, Family Futures will consider whether the child is mature enough to understand their rights. If FF is confident that the child can understand their rights, then we will respond to the child rather than a parent. What matters 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. When considering borderline cases, FF will take into account, among other things:

- the child's level of maturity and their ability to make decisions like 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.

It does not follow that, just because a child has capacity to make a subject access request, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so.

Charging

The information is provided free of charge. However, Family Futures can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we can charge a reasonable fee taking into account the administrative costs of providing the information or refuse to respond.

Where we refuse to respond to a request, the requester will receive an explanation and be informed about their have the right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Disclosure of client data to third parties

Information on clients will not be disclosed to any third party without the informed consent of the client, unless the matter is regarded as a child protection issue.

Data must not on any account be disclosed over the telephone because the caller's identity can be difficult to verify. If you receive such a request you should ask the person to put the request in writing via letter or email.

Data can be disclosed to a third party without the consent of the data subject in the following circumstances only:

- Data required by law e.g. data supplied to statutory bodies.
- Data that is in the vital interests of the data subject
- Data that would prevent harm to a third party
- Data that would prevent crime
- Data that would be in the interest of national security.

A record must be kept on file of any disclosure, including date, to whom, and the reason for the request.

There may be circumstances where Family Futures is required either by law or in the best interests of our clients or staff to pass information onto external authorities such as local authorities. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Other Data Subject rights

Family Futures recognises the range of rights that Data Subjects have, and will respond promptly and appropriately.

Any staff member or volunteer who receives a request from a Data Subject to exercise any of their rights must pass this immediately to the Data Protection Lead who will provide the response.

Direct marketing

We use a range of marketing activities and channels to communicate with our supporters and clients: our website, social media, emailed newsletters, display stands at events and leaflets given out to supporters or prospective adopters.

These channels are used for updates about our services and products, to inform supporters and to gather information in the following ways:

- To provide information for prospective adopters about adopting a child with Family Futures
- To update supporters about Family Futures' work, assessment and therapy services, events, training, publications, research, campaigns and fundraising.
- To administer events and services we are providing, including keeping a record of payments made, and to record for our administrative purposes the supporter/client's relationship with us
- To manage communication preferences

- To obtain information, conduct research and gather feedback to improve Family Futures' services and user experiences.

For marketing purposes we will keep the following personal data (from May 2018) where the subscriber has opted in to receive updates from us:

- First name, last name, emails address, optional description (e.g. Adoptive parent, professional), source (where you heard about us) and mailing preferences.

This data will be collected via sign up on our website, or via a link to our Family Futures sign up form on Mailchimp.

For Training/Events purposes, personal details will be collected that are required for the administration of booked training courses and other events such as conferences or book launches. (i.e. name, job title, organisation, dietary preference, special requirements, fee paid, date/course attended.) We will retain details of course attendance for 6 years

For sales of publications, DVDs and downloads via the website, personal details for processing the purchase will be collected and stored securely.

Opting out

The opportunity to unsubscribe from the marketing mailing list will be given on every marketing email sent out via an 'unsubscribe' link.

Preferences will be recorded on the master list used for all marketing. There will only be one list on Mailchimp from May 2018 to ensure mailing preferences are adhered to and to avoid duplication of records.

If a client wishes to hear from us about the service but no longer wishes to receive marketing updates their details will be recorded as 'unsubscribed' on the marketing master list.

Any requests to 'unsubscribe' which do not come through the automated link to the mailing list should be forwarded to the Marketing & Communications Specialist, who is responsible for managing marketing mailing preferences. Our Privacy Policy states that requests to withdraw consent should be emailed to contact@familyfutures.co.uk or posted to Family Futures CIC, 3 & 4 Floral Place, 7-9 Northampton Grove, London N1 2PL. Any other 'unsubscribe' requests (verbal or written) that staff members are made aware of should be forwarded to the Marketing & Communications Specialist by email.

Sharing lists

Family Futures does not share any mailing lists or data that has been collected for marketing purposes with any third parties. The data is held securely on a password protected email management system (Mailchimp).

Policies covering Data Protection content

The following policies are available on our website and cover data protection.

Privacy https://www.familyfutures.co.uk/privacy-policy/

It is compulsory for people to read this when signing up to our mailing list.

Cookies/Disabling Cookies (part of Privacy Policy)

Terms and Conditions https://www.familyfutures.co.uk/terms-and-conditions/

Definitions

Data Controller

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act. It will almost always be the organisation, not an individual staff member or volunteer. Separate organisations (for example a charity and its trading company) are separate Data Controllers. Where organisations work in close partnership it may not be easy to identify the Data Controller. If in doubt, seek guidance from the Information Commissioner.

Data Processor

When work is outsourced, which involves the contracting organisation in having access to personal data, there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor, as long as the Processor has been following the Controller's instructions.

Personal data

Any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data

Information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Enforcement

The ICO has a range of corrective powers and sanctions to enforce the GDPR. These include issuing warnings and reprimands; imposing a temporary ban on data processing and ordering the rectification, restriction or erasure of data.

There are two tiers of administrative fines that can be levied:

- Up to €10 million, or 2% annual global turnover – whichever is higher
- Up to €20 million, or 4% annual global turnover – whichever is the higher.

The fines are based on the specific articles of the Regulation that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

Policy review	
Responsibility	The Data Protection Lead will carry out the next review
Procedure	The policy will be reviewed in consultation with the Services' Managers' Team, Marketing, Training, Assessment & Therapy Services admin staff and Business & Finance.
Timing	As the GDPR becomes law in May and some details won't become final until after that date, it will be necessary to amend the policy in the subsequent months.