Data Protection Policy (GDPR)

Contents

Definitions

Charity means Family2Family, a charitable organisation

GDPR means the General Data Protection Regulation.

Responsible Person means Leila Parker. However, overall and final responsibility for data protection lies with the management committee, who are responsible for overseeing activities and ensuring this policy is upheld. All volunteers are responsible for observing this policy, and related procedures, in all areas of their work for the group.

Register of Systems (GDPR Documentation Controller)
means a register of all systems or contexts in which personal data is processed by the Charity.

Personal Data is information about a person which is identifiable as being about them. It can be stored electronically or on paper and includes images and audio recordings as well as written information.

Data Protection is about how we, as an organisation, ensure we protect the rights and privacy of individuals, and comply with the law, when collecting, storing, using, amending, sharing, destroying or deleting personal data.

Privacy Policy See Appendix 1 for Family2Family's Privacy & Cookie policy.

Data Protection Principles
The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:
a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Therefore you have the following rights:
• Transparency over how we use your personal information (right to be informed).
• Request a copy of the information we hold about you, which will be provided to you within one month (right of access).
• Update or amend the information we hold about you if it is wrong (right of rectification).
• Ask us to stop using your information (right to restrict processing).
• Ask us to remove your personal information from our records (right to be 'forgotten').
• Object to the processing of your information for marketing purposes (right to object).
• Obtain and reuse your personal data for your own purposes (right to data portability).
• Not be subject to a decision when it is based on automated processing (automated decision making and profiling).

You can find out more about your rights under Data Protection Law by visiting The Information Commissioners Office website (www.ico.org.uk). Remember, you can change the way you hear from us or withdraw your permission for us to processing your personal data at any time by contacting us at hello@family2family.org.uk

General provisions
a. This policy applies to all personal data processed by the Charity.
b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner. See Right to Access Personal Data.

Lawful purposes

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests. See Lawful basis for processing.
b. The Charity shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

Data minimisation

a. The Charity shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate and kept up to date
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. Personal data shall be reviewed yearly, and if appropriate updated or removed. See Data Retention & Destruction Policy

Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why. See Data Retention & Destruction Policy
c. This section details your Right to Erasure

Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place. We use Dropbox which has it's own backup and DR procedures.

Breach
In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Specific Procedures
We collect personal data in connection with specific activities, such as campaign updates, feedback, donations, competition entries, fundraisers, information users provide by Social Media and referrals. The information is either needed to fulfill their request or to enable us to provide the best possible service. It will be made clear to them when this information is being requested and that they will not have to provide the information if they don't want to; however, this may mean we cannot fulfill their request.

Sometimes, with their consent, we will use their personal data to provide them with information about our work or our activities that they have previously shown interest in. On other occasions, we may process personal data when we need to do this to fulfill a contract (for example, if you they have been involved in Fundraising and we need to post a pack or item to them) or where we are required to do this by law or other regulations. Family2Family also processes their data when it is in our legitimate interests to do this and when these interests do not override your rights. Those legitimate interests (Ref: Lawful Purpose above) include providing you with information on our appeals, services, products, fundraising, newsletter requests, feedback, competitions and other activities.

Supporting individuals
- The data we collect about families we support (via professionals/service users) does not make them identifiable.
- From time to time, individuals contact Family2Family to ask us to help such as through provision of items or clothing. In this instance, individuals are redirected to access the service via referral from a professional and the correspondence deleted.
- Should it be necessary to contact a professional on their behalf, we will request explicit, written consent before sharing any personal details with the Local Authority or any other relevant third party.
- We will keep information relating to an individual personal because it is needed to justify grants and funding so we can show a demographic of where the funds go. This information does not make them identifiable.
- Details relating to individual's circumstances and needs will be treated as strictly confidential.
- Please also see our Confidentiality Policy on the disclosure of personal information relating to service users, families, volunteers & supporters

Fundraising
- To order fundraising packs, people contact us via email or social media and are given the option to receive a digital or printed pack. This involves providing a name, email and sometimes an address for the items to be delivered to.
- Details collected for this purpose will be deleted within one month of completion of the fundraiser and transfer of funds raised to our Family2Family Local Giving account. Contact details will not be used for any purpose other than communicating with them about their fundraising event. However, if people are connected via Social Media they will see any public posts until they choose to turn off the notifications or unfollow.

Contacting volunteers

- People can volunteer for Family2Family in a number of ways.
- We will maintain a list of contact details of our recent volunteers. We will share volunteering opportunities and requests for help with the people on this list.
- We will also let volunteers know of any changes that might affect them volunteering with us and which they need to be aware of.
- We will only use this information in relation to their volunteering with us and whilst they remain a volunteer with Family2Family.
- By agreeing to volunteer with Family2Family they are agreeing to us to sending emails (or other means of contact) about volunteering and their volunteer role(s).
- People will be removed from the list if they have not volunteered for the group for 12 months. However, if people are connected via Social Media they will see any public posts until they choose to turn off the notifications or unfollow
- When contacting people on this list, we will provide a privacy notice which explains why we have their information, what we are using it for, how long we will keep it, and that they can ask to have it deleted or amended at any time by contacting us.
- To allow volunteers to work together to organise for the group, it is sometimes necessary to share volunteer contact details with other volunteers e.g. in the process of organising an event you have chosen to attend. We will only do this with explicit consent.
- Please also see our Confidentiality Policy on the disclosure of personal information relating to service users, families, volunteers & supporters

Contacting committee members (Trustees)

- The committee needs to be in contact with one another in order to run the organisation effectively and ensure its legal obligations are met.
- Committee contact details will be shared among the committee.
- Committee members will not share each other's contact details with anyone outside of the committee, or use them for anything other than Family2Family business, without explicit consent.

Appendix 1: Privacy & Cookie Policy

This Privacy Policy applies to information we (Family2Family) collect about individuals who interact with our organisation. It explains what personal information we collect and how we use it. If you have any comments or questions about this notice, feel free to contact us at hello@family2family.org.uk

Personal data that we process

The following table explains the types of data we collect and the legal basis, under current data protection legislation, on which this data is processed.

Purpose	Data (Key Elements)	Basis
Enquiring about our organisation and it's work and/or how to donate or make a referral	Name, email / social media name, message	Legitimate interests – it is necessary for us to read and store your message so that we can respond
Becoming a volunteer	Name, email, phone number, address, emergency contact	Consent – you have given your active consent
Referee of a volunteer	Name, email, phone number, address	Legitimate interests – it is necessary for us to request a reference (the details provided by the prospective volunteer)
Making a referral (Referral Partners)	Referrer: Name, email, phone number, place of work and job title Family: Age / due date, gender, post code, reason for referral (tick box), items requested, additional information	Consent – you have given your active consent. Legitimate interests – this is for the purpose of screening our beneficiaries so we can support them in the best possible way and can evidence this when applying for funding/grants
Beds4Kids referral	Family name, contact number, address	Legitimate interests – details needed to process an online order and delivery via third party business so we can meet the need of the family. Consent given by family.
Feedback regarding a referral	Name, email	Consent – you have given your active consent
Subscribing to email updates about our work	Name, email	Consent – you have given your active consent
Liking or following our social media accounts	Name, social media handle / name	Consent – you have given your active consent
Making a physical donation	Name, email, social media name	Legitimate interests – this information is necessary to keep until the donation has been received so we can make contact in case of emergency office closures
Making a monetary donation	Name, email, address, payment information	Legitimate interests – this information is necessary for us to fulfil your intention of donating money and your expectation of receiving a confirmation message. *Processed via a third party*
Website Family2family.org.uk	Please see Cookies & usage tracking	
Fundraising Gala	Business supporter: Name, phone number, email, company, payment information Gala attendee: Name, email, payment information	Legitimate interests: having shown an interest in this fundraiser, we will keep this information for the following year unless you have explicitly asked to be removed Consent – you have given your active consent

How we use your data
We will only use your data in a manner that is appropriate considering the basis on which that data was collected, as set out in the table at the top of this policy.
For example, we may use your personal information to:
- reply to enquiries you send to us;
- handle donations (monetary or physical) or other transactions that you initiate;
- where you have specifically agreed to this, send you marketing communications by email relating to our work which we think may be of interest to you.

When we share your data
We will only pass your data to third parties in the following circumstances:
- you have provided your explicit consent for us to pass data to a named third party;
- we are using a third party purely for the purposes of processing data on our behalf and we have in place a data processing agreement with that third party that fulfils our legal obligations in relation to the use of third party data processors; or
- we are required by law to share your data.

In addition, we will only pass data to third parties outside of the EU where appropriate safeguards are in place as defined by Article 46 of the General Data Protection Regulation.

How long we keep your data
We take the principles of data minimisation and removal seriously and have internal policies in place to ensure that we only ever ask for the minimum amount of data for the associated purpose and delete that data promptly once it is no longer required. Where data is collected on the basis of consent, we will seek renewal of consent at least every three years.

Rights you have over your data
You have a range of rights over your data, which include the following:
- Where data processing is based on consent, you may revoke this consent at any time and we will make it as easy as possible for you to do this (for example by putting 'unsubscribe' links at the bottom of all our marketing emails).
- You have the right to ask for rectification and/or deletion of your information.
- You have the right of access to your information.
- You have the right to lodge a complaint with the Information Commissioner if you feel your rights have been infringed.

A full summary of your legal rights over your data can be found on the Information Commissioner's website here: https://ico.org.uk/

If you would like to access the rights listed above, or any other legal rights you have over your data under current legislation, please get in touch with us. Please note that relying on some of these rights, such as the right to deleting your data, will make it impossible for us to continue to deliver some services to you. However, where possible we will always try to allow the maximum access to your rights while continuing to deliver as many services to you as possible.

Cookies & usage tracking
A cookie is a small file of letters and numbers that is downloaded on to your computer when you visit a website. Cookies are used by many websites and can do a number of things, e.g. remembering your preferences, recording what you have put in your shopping basket, and counting the number of people looking at a website.

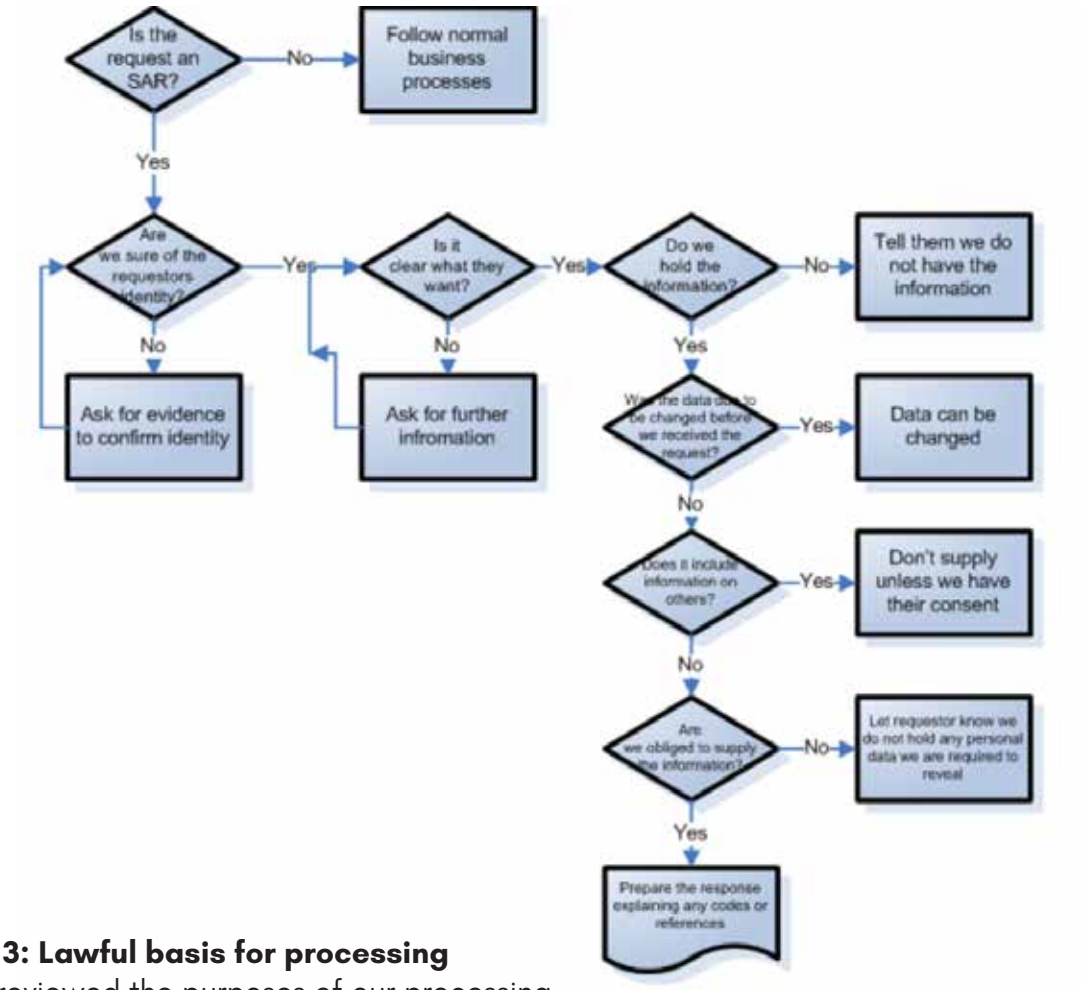
Our website is a WIX site, and collects some information about traffic to the site, but we do not collect data that makes users identifiable.
WIX Cookie Description:

Cookie Name	Purpose	Duration	Cookie Type
XSRF-TOKEN	Used for security reasons	Session	Essential
hs	Used for security reasons	Session	Essential
svSession	Used in connection with user login	12 months	Essential
bSession	Used for system effectiveness measurement	30 minutes	Essential

We may modify this Policy from time to time and will publish the most current version on our website. If a modification meaningfully reduces your rights, we notify people whose personal data we hold and is affected.

Blocking and Deleting Cookies
For more information about how to manage cookies, including blocking and deleting cookies please visit www.aboutcookies.org or www.allaboutcookies.org. Please note blocking all cookies may have a negative impact upon the usability of many websites.

Appendix 2: Right to Access Personal Data
Right to Access Personal Data / Subject Access Request (SAR) Process



Appendix 3: Lawful basis for processing

- We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.
- The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

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

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

- The GDPR Documentation Controller shows the full details of what we collect and why
- We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable way to achieve that purpose.
- We have documented our decision on which lawful basis applies to help us demonstrate compliance.
- We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- We will not be processing category data of individuals (race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.)

Appendix 4: Data Retention & Destruction Policy

The purpose of this Policy is to ensure that necessary records and documents of Family2Family are adequately protected and maintained and to ensure records that are no longer needed or are of no value are discarded at the proper time in the proper manner. This policy applies to all records generated in the course of referrals and volunteers, including both original documents and reproductions.

Type of Data	Retention Period	Reason for length of period	Accountable Person
Financial			
Accounting records related to income and expenditure	6 years from the end of the financial year the transaction was made.	Companies Act/Charities Act/HMRC requirements	Treasurer
Gift Aid declarations	To be retained whilst in use and destroyed 6 years after it is no longer required.	HM Revenue & Customs	Treasurer
Successful quotations for capital expenditure	Permanently	Commercial considerations	Treasurer
Invoice for a capital item	To be retained whilst the capital item is still in use and destroyed 6 years after the capital item has been removed from the fixed asset.	Companies Act/Charities Act/HMRC requirements	Treasurer
Contract with customers, suppliers or agents, licensing agreements, rental/hire purchase agreements, indemnities and guarantees and other agreements or contracts	6 years following the end of the contract or the end of the accounting year whichever is later.	Limitations Act 1980	Treasurer
Annual Accounts and Annual Report	Permanently	Data Protection Act	Treasurer
Balance sheet items, e.g. current assets and liabilities	Retained whilst current and then destroyed 6 years from the end of the financial year of the last transaction	Companies Act, Charities Act, HMRC requirements	Treasurer
Fixed Assets Register	Permanently	Companies Act, Charities Act, Commercial	Treasurer
Service User Correspondance			
Contact and personal information related to service users	Permanently, marked inactive following 6 months of inactivity	Data retained to provide evidence of usage with the service user	Chair
Referral forms/details of families nb no families are identifiable from the data provided	Permanently	Organisational benefit, evidence need by location/vulnerability	Chair
Volunteer Records			
Personnel files, including training records, supervision notes, and all other	6 years after volunteering ceases	Limitations Act 1980	Secretary

documentation related to volunteering. This excludes any problem solving records.			
Expenses & overtime records	6 years after volunteering ceases	Taxes Management Act	Treasurer
Applications forms and interview notes (for unsuccessful volunteers)	1 month following the closing date	Disability Discrimination Act 1995 and Race Relations Act 1976.	Secretary
Records relating to volunteering time	2 years from date on which they were made	The Working Time Regulations	Secretary
Insurance			
Insurance Policies	3 years after lapse	Data Protection Act	Chair
Claim Correspondence	3 years after settlement	Data Protection Act	Chair
Supporter, Events and Promotional Information			
Contact and personal information related to volunteers	6 years following the end of their volunteer role	Limitations Act 1980	Secretary
Meeting Minutes	Permanently	For 7 years to evidence financial decisions and thereafter for historical purposes.	Secretary
Compliance/Reporting information			
Register of Complaints/Safeguarding/ Data Protection Breaches, including relevant correspondence	10 years	National Archives guidance	Chair
Board of Trustees Meeting Minutes	Permanently	Companies Act/Charities Act/Data Protection Act	Secretary
Internal meeting minutes	3 years	Organisational benefit	Secretary
Approved Policies	3 years after being superseded	Limitations Act 1980	Secretary
Funding Applications			
Grant applications	To be reviewed after 20 years*	Organisational benefit	Chair
Monitoring reports	To be reviewed after 20 years*	Organisational benefit	Treasurer
General correspondence			
Routine correspondence that requires no follow up or is considered to be a general enquiry	1month	Organisational benefit	All
Documentation related to internal processes	1 year after superseded	Organisational benefit	All

Data Destruction
Personal data is removed, deleted or destroyed as appropriate with integrity and confidentiality, please see the security section set out in the General Data Protection Policy.

- When removing, returning, deleting or destroying any personal data, every reasonable and affordable step is taken to ensure it is done in a manner which is secure and ensures privacy; thereby keeping the risk of theft, loss or interception to an absolute minimum.
- Appropriate and proper tools and processes must always be used.
- If personal data can be anonymised/pseudonymised, care must be taken to ensure that:
- Duplications are identified.
- Historical versions are identified e.g. in computer history
- Versions held in backup files or servers are identified.
- Only a justifiable number of historical copies are retained and that any copies which may be deleted or removed are done so securely. Access to retained copies should be restricted to only those who absolutely require access at all times. Additional occasional access may be granted to others when and only for as long as access is required.
- When returning or sending any personal data, it must be moved in a way which is secure and ensures privacy; such that the risk of theft, loss or interception is kept to a minimum. It must also be returned in a commonly used format. For example, HMRC returns will be via secure internet portal. Accounts will be via secure digital link. Emailing will be kept to a minimum.
- Reasonable steps should be taken to verify the identity of the recipient. For example, two forms of communication may be used such as making a telephone call to the recipient ahead of sending the information to a known e-mail address.
- If it is necessary to destroy personal data or delete it irrevocably, then professional advice must be sought for example from an IT specialist. The must be notified of any intentions such as this in order to oversee the process.
- If personal data is ever removed, deleted or destroyed accidentally or without authorisation of the Controller, it must be reported in accordance with the Personal Data Breach Procedure.
- On occasion it may be necessary to retain evidence of the removal, deletion or destruction of personal data, particularly when the data subject has requested information regarding the erasure or has asserted the right to be forgotten.
- If we receive a request to have personal data erased or forgotten in accordance with a data subjects statutory right, then we may need to inform any recipients of that data so that the recipient may make steps to remove, return, delete or destroy the data as appropriate.

Appendix 5: Right to Erasure
Preparing for requests for erasure
- We know how to recognise a request for erasure, and we understand when the right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for erasure
- We have processes in place to ensure that we respond to a request for erasure without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.
- We have procedures in place to inform any recipients if we erase any data we have shared with them.
- We have appropriate methods in place to erase information.

Record requests we receive verbally

These will be logged in this document: Right to Erasure – Verbal Request Log

A request for erasure

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

Appendix 6: Security

- Our main website does not use cookies and it does no processing
- We undertake an analysis of the risks presented by any processing we/our third parties need to do and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- Our third parties process our information: jotform, wix, appointlet and dropbox
- The jotform contact forms are sent on a secure SSL certified platform and uses a HSA256 certificate
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We understand the requirements of confidentiality, integrity and availability for the personal data we/our partners process.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

Appendix 7: Confidentiality Policy

Confidentiality Policy on the disclosure of personal information relating to service users, families, staff, volunteers & supporters

The confidentiality policy sets out Family2Family's practices and procedures on the disclosure of personal information relating to service users, families they support, staff, volunteers and supporters. This policy is there to protect the interests of our service users and to ensure that they can have trust and confidence in Family2Family. It also protects Family2Family, its trustees, staff and volunteers and complies with data protection law (GDPR).

Reasons for this Policy Statement

- To protect the interests of our service users, families they support, our staff, volunteers and supporters
- To ensure all service users, families they support, our staff, volunteers and supporters have trust and confidence in Family2Family
- To protect Family2Family, its trustees and volunteers
- To comply with data protection law (GDPR)

Its meaning

- volunteers receiving personal information about services users and the families they are working on behalf of, other volunteers or supporters should treat this information as confidential.
- under no circumstances should staff and volunteers share personal information with their own partners, family or friends.

Family2Family will seek to ensure that:

- All personal information will be treated as confidential. Information will only be collected that is necessary and relevant to the work in hand. It will be stored securely, only accessible on a need to know basis to those volunteers duly authorised. The retention periods of personal information is covered in the retention section of the Data Protection Policy
- Where consent is not given for the Charity to record and store basic information about the service user it is unlikely that a service will be able to be provided.
- All information stored in Family2Family's Register of Systems will be kept secure and treated as confidential.
- Paper records (which will be limited) will be kept in a locked cabinet with restricted access.
- The signed consent form (where applicable) or the noted consent (and where it came from) will be stored in Dropbox (if appropriate) and referred to in the Register of Systems.
- All service users are made aware of their right of access to their records.
- Every effort will be made to ensure the physical environment in which face to face discussions and telephone conversations take place does not compromise family confidentiality.
- Service users will be made aware of their right to complain if they feel confidentiality has been breached.
- Breaches of confidentiality will be dealt with through the Family2Family's volunteer disciplinary procedures

Notes:

By personal information we mean both:

- The data protection definition which is any information which enables a living person to be identified (e.g. name, address, phone number, email address, or Special Categories of Personal Data which requires the individual's explicit consent for it to be held by Family2Family, e.g. ethnicity, sexual life, political interests, religious beliefs, trade union affiliations etc.
- Information, written or verbal, about a family that relates to their circumstances that is provided to you for context so that you can provide a personalised service

- The data we collect about families we support does not make them identifiable.
- From time to time, individuals contact Family2Family to ask us to help such as through provision of items or clothing. In this instance, individuals are redirected to access the service via referral from a professional and the correspondence deleted.
- Should it be necessary to contact a professional on their behalf, we will request explicit, written consent before sharing any personal details with the Local Authority or any other relevant third party (unless there is a safeguarding concern)