Family Counselling Trust

Privacy Policy

Table of Contents

Introduction

The Family Counselling Trust is a charity that offers a grant-supported service for children, young people and families where there are emotional, behavioural or other mental health problems. The charity provides families with concerns about their children's behaviour, emotions and family relationships with information, advice and guidance on what counselling can achieve and offers counselling as appropriate in consultation with the family. The charity needs to collect and use information on individuals such as children, young people, parents or guardians, donors, volunteers, practitioners, educational and healthcare professionals and staff members.

We use this information to manage the charity, deliver our services and raise money. However, we must ensure we use and protect the information in accordance with current legislation. Failure to do so could lead to distress to individuals, financial sanctions from the Information Commissioner's Office (ICO), reputational damage and impair our ability to raise funds and continue with our charitable activity.

This policy describes how we will protect personal information to safeguard the individual and comply with the law.

Definitions

Data Controller

Family Counselling Trust is the data controller and we are registered with the ICO. We are responsible for all the personal information we collect.

Data Subject

The data subjects are the individuals whose personal information we deal with such as children, young people, parents or guardians, donors, volunteers and staff members.

Personal Information

Personal information means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, from the personal information held. The information includes name, address, date of birth, email, telephone number, national insurance number etc. Personal information also includes information associated with that individual such as financial information of donors, medical records and staff development, staff reviews and pay rates.

Sensitive information such as medical, race, religion, sexuality, political or trade union membership are a special category of data that requires sensitive handling.

Data Processing:

Processing means any action performed on personal information, which includes collection, recording, organising, storing, sharing and transmitting. This includes electronic and paper documents containing personal information. Many of the activities within the charity involves processing information and therefore we must comply with the law.

Legislation

The charity must comply with the Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR). The GDPR came into full force on 25 May 2018 and carries much larger sanctions for any breaches.

Governance

Roles and Responsibility

Everyone associated with Family Counselling Trust has a responsibility to ensure we protect the personal information we hold and comply with this policy.

Board Level

Peter Barrowcliff, Family Counselling Trust Treasurer, is the Data Privacy Manager and is accountable to the board of trustees for data privacy and will report at least annually to the board on data privacy at board meetings.

Privacy Officer

Each county has a Privacy Officer who has day-to-day responsibility for data privacy, and is the main point of contact for any questions about data privacy. The contacts for the Privacy Officers are as follows.

Dorset:	Eliza Modzelewska	email: elizamodzelewska@gmail.com
Hampshire:	Peter Currie	email: apncurrie@icloud.com
Somerset:	Claire Davey at	email: fctsomerset@gmail.com
Wiltshire:	Cyndy Walker at	email: fctwflora@outlook.com

Staff Responsibilities

All staff and volunteers are responsible for complying with this policy.

Review of Policy

The Board with review this policy annually.

Risk Management

Data Privacy Impact Assessment (DPIA)

When we are considering processing information in new way or using a new technology, such as hosting personal information in the cloud or using a mobile phone application to process personal information, the Privacy Manager will decide whether a Data Privacy Impact Assessment (DPIA) is required.

Risk Register

The Privacy Manager will maintain a risk register of the charity's data protection risks. The register will be reviewed annually by the board of trustees.

Privacy Principles

Collecting Information

We should collect the minimum information we need to complete a task. We should not collect information just in case. If someone is making an enquiry about our services we should only collect their name and contact details. If they wish to apply for our services further information can be collected at this point.

Where we receive a referral from another organisation i.e. school or healthcare professional we must contact the data subject or the parent/guardian and confirm that we now hold their information and what we intend to do with it, and ensure a copy of the Privacy Notice is provided.

Processing Information

When we are planning to process information, we need to consider whether we need the individual's consent to process. The majority of our processing is for legitimate business reasons to run our charity; we need to pay staff, process donations, share information with practitioners, and therefore we do not require consent. However, some activities may not be considered legitimate business. We must obtain and record consent for this type of processing and renew it every three years.

Securing Information

We must protect the personal information we use whether in electronic or paper format.

- Documents containing personal information should be stored in a secure cabinet or container when not required.
- Documents containing volunteers, families' referral information should only be removed from secure devices, cabinets or containers where necessary. Documents must be protected while out of stored equipment and should not be left unattended.
- Electronic copies of personal information must be stored on secure password protected devices.
- Electronic documents if emailed to home computers should have all personal identifiable information removed or password protected.
- Volunteers should not download electronic documents containing volunteers or families' information on their own devices unless password protected.
- When emailing referral personal information to third parties, such as practitioners, the information should be in a document that is password protected. Password to be sent via text, phone or other method.

Deleting data and data retention

When personal information is no longer required, and there is no legal requirement to retain the information, electronic data must be deleted and paper copies securely destroyed. Personal information will be held for not more than 7 years after it was collected, confirmed or updated.

Third Parties

When sharing personal referral information with third parties, such as practitioners, a contract must be in place which includes appropriate privacy clauses.

Subject Access Request

Individuals have the right to know whether we store and process their personal information, this is known as a Subject Access Request. If the information we hold is inaccurate they have the right for that information to be corrected. In certain circumstances, they have the right to have the information deleted or to be give a copy of that information. We will respond politely to any requests as soon as possible but in any event within one month. The individual does not have to state they are making a subject access request, it can be a simple email asking what information we hold, and therefore, any request by an individual with regards to the information we hold must be forwarded to the Privacy Officer.

We may require proof of identity before access is granted. The following forms of ID will be required: Driving license and/or passport.

FCT reserves the right to withhold confidential information from a parent who has requested access to his/her child's records if FCT has reason to believe this is not in the child's best interest and that the health and welfare of the child need safeguarding.

In the case of a parent, who is separated or divorced from the parent who is the main carer for the child, and who is requesting access to information held about the child, evidence of Parental Responsibility may be required before access is granted

Communication

Family Counselling Trust is registered with the ICO as a data controller and data processor. The Privacy Manager is responsible for maintaining our registration.

We will have a privacy notice which will clearly inform individuals how we collect their information, what we do with their information and their rights. A copy of the relevant privacy notice will be displayed prominently on our website and a copy will be sent to individuals when we are requesting information from them.

The Privacy Manager is responsible for maintaining the privacy notice.

Education and Awareness

All new joiners including volunteers and temporary staff must read this data privacy policy as part of their induction process.

All staff and volunteers will receive data privacy training as appropriate.

The Privacy Manager will periodically send emails to all volunteers, practitioners and family liaison officers highlighting key aspects of data privacy.

Incident Handling

We have a legal responsibility to report certain data privacy incidents to the ICO within 72 hours or face a financial penalty. It is essential all staff and volunteers follow the incident procedure. Example of privacy breaches are:

- Emailing children and families personal referral information to a wrong person.
- Revealing contact details to an unauthorised third party.
- Leaving personal therapy notes unsecured in a public area.
- Losing a laptop or tablet containing the personal information of children and families.

Not all the examples above are reportable to the ICO however it is essential that staff and volunteers report any incident or potential incident to the Privacy Officer. The Privacy Manager will then discuss with the Privacy Officer and decide whether the incident requires reporting to the ICO and whether an action is required to manage the risks from the incident.

Assurance and compliance

The Privacy Manager will carry out periodic checks to monitor volunteers' compliance with this policy.