The Suffolk Parent Carer Forum Data Protection Policy

As an organisation we need to collect and use certain types of information about the different people we come into contact with in order to carry out our work.

Suffolk Parent Carer Forum (SPCF) is committed to protecting and respecting the personal information we collect, process and store.

This policy applies to all management committee members, parent representatives and volunteers. Any breach of this policy will be viewed as a disciplinary matter.

Definitions

Personal Data: any information which enables a person to be identified.
Sensitive data: a specific set of special categories that must be treated with extra security.
Data Subject: an individual about whom data is held (e.g. SPCF members, staff and volunteers)
Data Controller: entity with overall responsibility for data collection and management (Suffolk Parent Carer Forum trustees and staff)
Data Processor: an individual handling or processing data (SPCF management committee, parent representatives and volunteers)
Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed.

Background & Legislation

The General Data Protection Regulations (GDPR) came into effect in the UK on 25 May 2018. The regulations give individuals the right to know what information is held about them and provide a framework to ensure that personal information is handled properly.

SPCF is committed to collecting and processing data in accordance with the principles set out the GDPR which require that personal information is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary kept up to date.
- 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.
- 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.

SPCF is committed to complying with the GDPR principles at all times. This means that we will:

- Inform individuals as to the purpose of collecting any information from them, as and when we ask for it.
- Be responsible for checking the quality and accuracy of the information and keeping it up to date.
- Regularly review our records to ensure that information is not held longer than is

necessary.
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or electronically, and follow the relevant security policies (SPCF Password Policy)
- Not share personal information with others unless there is a safeguarding, regulatory or legal requirement to do so
- Set out clear procedures for responding to requests for access to personal information
- Report any breaches of the GDPR in accordance with the procedure set out below.

Confidentiality and Sharing Information

Because confidentiality applies to a much wider range of information than Data Protection, we have a separate Confidentiality Policy. This Data Protection Policy should be read in conjunction with the Confidentiality Policy.

All personal information will be regarded as confidential and will not be shared without an individual's knowledge or consent, except:
- Where SPCF is legally bound to provide information.
- To provide some services with other agencies (Third Party Agreement).
- Statistical information used for research and monitoring purposes.

Data Storage, Security and Retention

Any recorded information on members, volunteers and employees will be:
- Handled, transferred, processed and stored with the utmost care and regard
- Stored in secure office facilities, locked drawers or cabinets, or secure cloud-based digital storage.
- Protected by the use of passwords if kept on computers and/or other devices and encrypted if appropriate.
- Destroyed confidentially if it is no longer needed, or if requested by an individual.

We will regularly review our procedures for ensuring that our records remain accurate and consistent.

Information will be stored for only as long as it is needed or required by statute. Paper records will be destroyed within six years of the individual they relate to ceasing contact with SPCF.

When the young person(s) that a member cares for reaches the age of 25 years, SPCF will contact them to confirm that they would like to stay on the database with the understanding that they will not have access to funded training. If the member declines the offer SPCF will send the family an exit letter referring them on to adult support groups and the Carers Centre where appropriate, and their details will be removed from the membership database.

SPCF will check the membership database once a year to identify members whose cared-for person is over the age of 25 years.

Access to Data

Information and records will be stored securely and will only be accessible to authorised employees and volunteers, and the individual to whom the information relates.

All individuals have the right to request access to personal information stored about them.

Individuals can contact SPCF at any time to request to see, change/correct and delete (where there is no good reason for us to continue to hold or process) the information we hold about them. SPCF will act on access requests within one month of receipt and will not charge for this.

Where the individual making a request is not personally known to SPCF, their identity will be verified before handing over any information.

Data Breaches

All Staff, trustees and volunteers are required to report any data breach to the Management Committee as soon as possible once they are aware that it has occurred.

Less serious breaches will be recorded and listed in an appropriate place, and trends or lessons learned will be reviewed.

Serious personal data breaches will be reported to the ICO within 72 hours of the breach occurring if possible, and if not, informing the ICO about the reasons for any delay.

Transparency

We are committed to ensuring that individuals are made aware of how and why their personal information is stored and processed, what types of disclosure are likely and how to exercise their rights in relation to the data.

Individuals will be informed in the following ways:

- Employees in the staff terms and conditions.
- Volunteers: in the volunteer induction pack.
- Trustees: in the roles and responsibilities/induction pack.
- Members: when they provide their information and consent to retain it is obtained, or when they request services (on paper, online or by phone).

Consent

Consent will always be sought prior to the storing and processing of data, and records kept of the dates, and circumstances. Online consent will be requested when clients sign up to services, donate or sign up to mailing lists. In all cases it will be documented on the database that consent has been given.

We acknowledge that, once given, consent can be withdrawn at any time.

Personal Information will only be made public with the individual's explicit consent. This includes photographs.

Consent will be obtained from parents, if children's data is being stored or processed depending on the age of the child/young person in accordance with legislation.

'Sensitive' data (including health information and ethnicity) will be held only with the knowledge and consent of the individual.

Sharing Information

SPCF will not normally share any information about individuals with any other agency without their consent. However, information sharing may take place without the consent or the knowledge of the individual concerned in the following circumstances:

- Where there are safeguarding concerns (see SPCF Confidentiality Policy and Safeguarding Policy).
- Where SPCF is legally bound to provide information, no consent need be sought, nor will individuals necessarily be informed that the information has been provided.
- Statistical or other anonymised information may be shared, for research and other purposes (e.g. with funders)
- Anonymised parent feedback is collated and reported to other agencies (e.g. Suffolk County Council, Suffolk CCG) to inform the design, planning and review of services.

Website

SPCF collects information from users of its website when they fill out a membership form or use an enquiry form.

The SPCF website uses cookies in order to enhance the experience of users by:

1. Tracking visitor statistics using Google Analytics.
2. Allowing users to share content on various social network sites.

The SPCF website contains links to other websites. These third-party sites have separate and independent privacy policies. SPCF therefore has no responsibility or liability for the content and activities of these linked sites.

Comments posted on SPCF's Facebook page are not moderated prior to publication. SPCF reserves the right to take action regarding comments which do not comply with the requirements of our Social Media policy. Action may range from simply deleting a comment and providing a warning, up to and including banning a user from future commenting privileges.

Third-Party Agreements

SPCF uses third parties to store/process data such as: event booking, online payments, cloud storage facilities, newsletter mailshots.

There should be a third-party written agreement with the other organisation to confirm they are meeting the regulations.
Third-party data needs to be stored on European servers to ensure they comply with GDPR.

Agreement

I have received a copy of the Data Protection policy and I have read, understood and agree to follow its content.

Signed: Date:

Print: