Data Protection Policy

Principles

Staffordshire Parent Carer Forum (herein referred to as the StaffsPCF) fully comply with the Data Protection Act 2018 and the data protection principles. We will adhere to the following principles:

- data must be processed and used fairly, lawfully and transparently for individuals.
- data must be collected and used for specified, explicit and legitimate purposes, and should not be processed further in a manner that is incompatible with those purposes.
- Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Data must be 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.
- Data must not be kept for no longer than is necessary
- Data must be handled and processed in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the organisation will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018
- take appropriate technical and organisational security measures to safeguard personal information

- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

Adherence to the policy

It is a requirement of membership of the StaffsPCF Steering Committee that all members must adhere to the policy. Failure to follow the Data Protection Policy may lead, therefore, to the curtailment of the volunteering/membership arrangement, and the possible withdrawal of future volunteering/membership opportunities with StaffsPCF

Definitions

The Data Controller is the legal 'person', or organisation, that determines the purposes and means of collecting personal data. The data controller is responsible for complying with the Data Protection Regulations 2018. Staffordshire Parent Carer Forum is the Data Controller and is registered with the Information Commissioner as such.

The Data Processor is the person responsible for processing data on behalf of the controller and has to comply with specific legal obligations. This can be different personnel according to which data we are concerned with.

The Data Subject is the individual whose personal data is being processed. Examples include members, reps, volunteers & member organisations, project beneficiaries and some suppliers.

Processing means the use made of personal data including:

• collecting and retrieving

• storing, whether in hard copy or electronically, and including backup copies

• accessing, using (sorting/analysing) or sharing, including outside of the organisation

• disposing of

Data Controller

The Data Protection Officer has the following responsibilities:-

- Reviewing data protection and related policies
- Advising the Steering Group on data protection issues
- Ensuring that security of electronic or paper personal or sensitive information is robust
- Handing subject access requests

All individuals who have access to personal or sensitive data, including any external data controllers, must:

- Read and understand the data protection policy
- Adhere to security measures described
- Not disclose any personal or sensitive information unless authorised to do so. The only exceptions relate to matters of safeguarding or criminality.

General Data Security

All Steering group Members are responsible for ensuring that:

- Any third party personal data they hold or process is kept securely.
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- In all activities involving third party personal data that all of the requirements of the GDPR as defined above are adhered to.
- Where they are uncertain of requirements or they suspect a data breach, reference should be made to the nominated GDPR data controller in the first instance.

Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected. Laptop users should not save any personal information to the local hard drive (i.e. C: drive) and should only save on to the SPCF shared drive.

Subject Consent

The Data Protection Act sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed.

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following:

- **Consent**: Genuine consent that offers individuals real choice and control
- **Contract**: if processing someone's personal data is necessary to fulfil the organisation's contractual obligations to them (eg to provide a quote).
- **Legal obligation**: if processing personal data is necessary to comply with a common law or statutory obligation.

- **Vital interests**: not one that will occur often as it refers to processing personal data to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent.
- **Legitimate interests**: the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

All data processing within StaffsPCF will be assessed against these bases.

Subject Access Requests

Any member of SPCF (for whom data is held) may request details of personal information which the organisation holds about him or her under the Data Protection Act. If a member would like a copy of the information held on him or her, they should write to info@staffspcf.co.uk

The requested information will be provided within one month. If there is any reason for delay, that will be communicated within the four-week period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If a member believes that any information held on him or her is incorrect or incomplete, then they should write to info@staffspcf.co.uk as soon as possible. StaffsPCF will promptly correct any information found to be incorrect.

Disposal of Data

StaffsPCF must ensure documents and data are retained for the time required by the law, regulators, insurers or by funders and then securely and properly disposed of.

Those listed in blue are governed by the data protection act as they directly relate to or could include significant amounts of personal data

Data category	Retention and disposal instructions
Member & Service related	
Membership and related records	Paper copies to be **retained only for period of active casework/support** and then added to electronic database and paper destroyed as confidential waste. Electronic records to be **cleansed annually** and **un-contactable deleted after 1 year of no contact or membership withdrawal**.

	Non-personal data can be retained for as long as reasonable useful
Data capture, survey and consultation data	Paper copies to be **retained only for period of data entry** and then destroyed as confidential waste. Electronic data capture records to be **cleansed annually**. Generic, non-personal survey data can be retained for as long as reasonably useful.
Training records	**Check specific dates** with funders and awarding bodies; otherwise destroy all paper records once details have been stored electronically.
Parent reps/Steering Group personal data	Paper copies to be **retained only for period of active casework/support** and then added to electronic database and paper destroyed as confidential waste. Electronic records to be **cleansed annually** and **un-contactable deleted after 3 years of no contact**.
Project specific records	Project records/reports – see specific funder, otherwise 2 years after project completion as confidential waste.
Organisational records, Partnership/forum meetings – including annual reports, accounts, Steering Group minutes, register of interests, agendas and minutes	Retained centrally and electronically. Dispose after 7 previous years have passed.

Data Breaches and Notification

The data protection act introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioners Office (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

In deciding whether it is a notifiable breach StaffsPCF will need to establish the likelihood and severity of the resulting risk to people rights and freedoms. If it's likely there will be a risk then we will notify the ICO. Even where we are not required to notify we still need to be able to justify the decision. For this reason we will keep a record of any personal data breaches, regardless of whether we are required to notify.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay.

All data breaches must be reported in the first instance to the Data Controller who will decide whether the breach is notifiable.

Date first agreed:	05/10/2021
Agreed by:	SPCF Steering Group
Reviewed On:	12/06/2025
Next review date:	12/06/2027