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 (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- 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.

This policy shall apply to any third party organisation subcontracted to perform any part or all of the process.

Data Protection Officer and 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

Data Controllers

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.

By 'special categories' we mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data about a person's sex life or sexual orientation.

Steering Group Member Personal Data

All Steering group members are responsible for:

- Checking that any information that they provide to the organisation in connection with their volunteering/membership is accurate and up to date.

- Informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of the volunteering engagement or subsequently. The organisation cannot be held responsible for any errors unless the volunteer has informed it of such changes.

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/data protection officer in the first instance.

Personal information should be kept in a locked filing cabinet, drawer, or safe.

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:

- **Contract**: if processing someone's personal data is necessary to fulfil the organisation's contractual obligations to them (e.g. 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

Any member of StaffsPCF (for whom data is held) may request details of personal information which the organisation holds about them under the Data Protection Act. If a member would like a copy of the information held on them, 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 time 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 them 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

Personal and sensitive information will only be kept for 18 months after membership of StaffsPCF has lapsed, or the time required by the law or by funders, after which data will be disposed of securely.

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 Protection Officer who will decide whether the breach is notifiable.

Date first agreed:	Click here to enter text.
Agreed by:	Click here to enter text.
Next review date:	Click here to enter text.