



Data Protection Policy and Procedures

POSCH (Parents and Carers of Special Children)

1. Policy statement
2. Procedure
3. Informed consent form
4. Code of conduct

POSCH is committed to a policy of protecting the rights and privacy of individuals. This policy applies to anyone working for or volunteering or subcontracted with POSCH. POSCH needs to collect and use certain types of data in order to carry on our work. This personal information must be collected and dealt with appropriately. Confidentiality is taken very seriously and we require everyone to abide by the organisations code of conduct and agree to no passing verbal or written information without consent or unless it's on need to know basis that identifies or names any individuals accessing the group past or present.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computer or in a manual file, and includes email, minutes of meetings, and photographs. POSCH as an organisation will remain the data controller for the information held, however a named data controller will also be designated. The staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

Trustee board members and volunteers or staff running the group who have access to personal information, will be expected to read and comply with this policy. Information regarding this will be provided at induction and made an ongoing supervision and training concern.

Purpose

The purpose of this policy is to set out the commitment and procedures for protecting personal data. POSCH regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The Data Protection Act Legislation

This contains 8 principles for processing personal data with which POSCH will comply. Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)



4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information POSCH will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998

Data Subject/Service User – The individual whose personal information is being held or processed by POSCH (for example: a service user or a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

- A. racial or ethnic origin of the data subject
- B. political opinions
- C. religious beliefs or other beliefs of a similar nature
- D. trade union membership
- E. physical or mental health or condition
- F. sexual orientation
- G. criminal record
- H. proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioners Office (ICO) about the data processing activities of the [Group]. Note: Not-for-profit organisations are exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.



Processing - Means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Group.

Applying the Data Protection Act within POSCH

Whilst access to personal information is limited to the staff and volunteers at the group Volunteers at POSCH may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Correcting Data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them.

Responsibilities

POSCH is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The board of trustees will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
 - The right to be informed that processing is being undertaken
 - The right of access to one's personal information



- The right to prevent processing in certain circumstances

- The right to correct, rectify, block or erase information which is regarded as wrong information

- Take appropriate technical and organisational security measures to safeguard personal information,

- Ensure that personal information is not transferred abroad without suitable safeguards,

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

- Set out clear procedures for responding to requests for information

The Data Protection Officer on the trustee board is:

Name ____Andrea Hobbs_____

Contact Details __andrea.hobbs027@gmail.com_____

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice

- Everyone processing personal information is appropriately trained to do so

- Everyone processing personal information is appropriately supervised

- Anybody wanting to make enquiries about handling personal information knows what to do

- Dealing promptly and courteously with any enquiries about handling personal information

- Describing clearly how it handles personal information



- Regularly reviewing and auditing the ways it holds, manages and uses personal information
- Regularly assessing and evaluating its methods and performance in relation to handling personal information
- Ensuring that all staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact POSCH Data Protection Officer.

Data collection

Informed consent

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

POSCH will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. POSCH will also speak explicitly about this to group users and ask them to consent to data collection (see appendix)

When collecting data, POSCH will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed



- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is the responsibility of POSCH to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Data Subject Access Requests

Members of the public may request certain information from the Local Authority under the **Freedom of Information Act 2000**. The Act does not apply to POSCH. However if at any time we undertake the delivery of services under contracts with the Local Authority we may be required to assist them to meet the Freedom of Information Act request where we hold information on their behalf.

Disclosure

POSCH may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows POSCH to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person



3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

POSCH regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

POSCH intends to ensure that personal information is treated lawfully and correctly.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of POSCH is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data.

Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of administering the campaign/project and securely dispose of once the promotion and monitoring period is complete. If a group user receives regular visits from a volunteer – ensure the list is securely stored and remove customer details when they change or the group user no longer receives the service. Review the list annually. We will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to POSCH please contact the Data Protection Officer (named above):

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.



Review

POSCH will ensure that issues of Data protection receive continuous attention and will regularly review the way that we operate to support this principle. This policy should be reviewed every 2 to 3 years or if the law changes.

Date approved: October 2017

Date of next review: October 2019

Signed: _____ Andrea Hobbs _____

Dated: _____ 8/12/2017 _____



POSCH acknowledges that in the process of providing a service people who use the service need reassurance that the information they provide is treated appropriately and not shared with others, and is maintained in a confidential manner.

We need to keep information to;

- Ensure that the services we provide will meet parent/carers and their family's needs
- Make sure that we provide services and activities safely.
- Work with other agencies, funders and stakeholders involved to plan what is provided.

We need to share information with;

- Staff who 'need to know' that information as part of providing good services.
- Any personal data obtained or used by any of the Parties in the course of the group's activity shall be processed in accordance with the Data Protection Act 1998.

The only personal data held by any party will be data which is relevant to the group's activities

- When POSCH has to work with other agencies, this is done with the knowledge and agreement of the child/young person and family concerned, and information is only shared on the basis of what the other agency 'needs to know'.
- POSCH will respect confidentiality when this is requested by a child who is competent to make their own decision, unless there are over-riding safety concerns.

Confidentiality Agreement

If POSCH staff or volunteers are concerned that a child may be being abused or is at risk of harm, a referral will be made to the local Children's Safeguarding Services. In most cases, the parents (and where appropriate, the child) will be told that this is being done.

In very extreme circumstances, a referral will be made to Children's Safeguarding Services without telling the parents that this is being done, if it is believed that telling them would place the child in more danger.

How will POSCH keep information safe and secure?

Access to documents stored electronically is password protected to ensure that only appropriate people can read it.

Lockable filing cabinets are provided for paper records, and systems are in place to keep these records safe at all times.

Staff are trained in the requirements of the Data Protection Act 1998

Personalised data will be collected with informed consent from the outset.

Therefore:

I agree to POSCH obtaining and holding information about me and my family in accordance with the above arrangements, and using that information for purposes stated above.

Signed:

Print name:

Date: