Brighton and Hove Speak Out

Policy: Confidentiality

Date agreed by Governance Board: 23rd Aug 2021

Staff annual review date: Aug 2022

Next Board review: Aug 2023

1. Why do we have a confidentiality policy?

This confidentiality policy is necessary to protect the people with learning disabilities who use Speak Out services, and our volunteers and staff from having personal information about them shared without their knowledge or consent. Speak Out also has a duty to follow data protection and confidentiality laws. It is essential that everyone feels safe while involved with Speak Out, either in an advocacy group, receiving 1-1 advocacy or while working or volunteering in any area of the organisation.

2. What do we mean by 'confidential'?

Keeping personal information confidential, means not sharing it with other people without permission from the person the information is about. It also means following policies and procedures to make sure that personal information is kept safe at all times and is not shared in error (e.g. by losing it, by having a weak password, or being overheard when talking).

3. What information is confidential?

Personal information is private information about a person. This information must not be shared with others without prior permission from that person (i.e. kept confidential).

4. Personal information includes:

- Personal data – e.g. Name and date of birth;
- Special category data – e.g. Race and gender;

- Any information shared in confidence where there is a common law duty of confidentiality – e.g. Record of a meeting with a service user, supervision notes, and personal reports.

Further details of these categories can be found in **Appendix A**. This policy will use the term 'personal information' to cover all of these categories.

All personal information about people involved with Speak Out is confidential unless they give permission for information about themselves to be shared.

However, staff and volunteers supporting people who use the project may need to discuss individuals with their supervisor. People with learning disabilities will be informed of this before they receive a service from Speak Out i.e. join an advocacy group or project or receive 1-1 support. Staff will share Speak Out's accessible confidentiality policy with all new services users.

5. Roles & Responsibilities

Accountable Officer

The **Data Protection Lead** (Speak Out's Director) will oversee the strategic and operational management of this confidentiality policy, including ensuring that the policy complies with all legal, statutory and good practice guidance requirements. The Data Protection Lead is also responsible for ensuring that the contracts of all staff and volunteers are compliant with the requirements of the policy and that confidentiality is included in staff and volunteer induction.

Speak Out Governance Board

A nominated Trustee from the Operations Subgroup of Speak Out's Governance Board will oversee any complaints or serious breaches relating to confidentiality.

Team Leaders

Team leaders are responsible for ensuring that this policy is built into working processes and that staff and volunteers comply with its content. Any breaches of this policy must be reported and investigated.

Staff and Volunteers

All staff and volunteers must follow this policy and maintain confidentiality. Any deliberate breach of confidentiality, inappropriate use of records, or abuse of computer systems may lead to disciplinary action being taken (see Speak Out's staff handbook and Volunteer Policy).

6. Explaining Confidentiality

Staff and volunteers will explain the Confidentiality Policy to service users at the initial meeting before they begin working with us. At the initial meeting, we will also obtain consent to hold personal information and to use it during the advocacy process. An Easy Read version of this policy is available to use as required.

The advocacy role requires us to share with service users all information received about them. Others (e.g. carers, social workers and support staff) may not be aware of this and assume

that we have a duty of confidentiality to them. Speak Out staff and volunteers may need to make others aware at the start of a conversation, that any information shared by them about a service user will be passed onto the service user in question.

Confidentiality will also be explained when a third party is involved in meeting to support communication with a service user (e.g. a community language interpreter, sign language interpreter or family member). The service users consent to their involvement will be sought and recorded.

7. Breaching Confidentiality

When personal information is shared without the persons consent, this is said to be a breach of confidentiality. A breach may occur intentionally or accidentally, or by loss, theft or system security error.

In the event of any accidental, negligent or wilful breach or possible breach of confidentiality, staff and volunteers must at the earliest opportunity report this to their line manager or another Speak Out manager (or the Volunteer Coordinator in the case of volunteers). All possible breaches will be promptly assessed, recorded and, where appropriate, reported to the Information Commissioners Office (ICO), in line with the Data Protection and Data Retention Policy. In such cases the relevant Trustee(s) will also be informed.

There are times however, when we need to share personal information without the person's consent. This could be to protect either their best interests or the interests of the wider public, for example to safeguard a person, or where a serious crime has been committed.

This means staff or volunteers may override your duty of confidentiality if they:

- Have information that suggests a client is at risk of serious harm.
- Have information to suggest that a client is posing a risk of serious harm to someone else.
- Have information that a serious crime is being committed.
- The service user is unable to consent due to lack of capacity, and a best interest decision has been made.

In these circumstances, staff or volunteers should always report concerns to a Speak Out manager. Staff and volunteers should follow the Safeguarding Adults and Children at Risk Policy and Procedures and Speak Out's Non-instructed Advocacy Policy, as appropriate. Written records must be kept in-line with these policies. Staff must fully support volunteers in these circumstances.

Sometimes circumstances are not always straightforward. If staff or volunteers have any concerns about someone, or if a confidentiality issue arises, they should always speak to a Speak Out manager for advice.

8. Confidentiality and Records

Records are kept by Speak Out to ensure effective working, accuracy and fairness.

The following information about service users will be kept on file:

- Key names and addresses
- Equalities monitoring data
- Advocacy plans, Build a Picture information or personal questionnaires
- Correspondence
- Case notes and a record of contact between themselves and Speak Out.

The following information about staff and volunteers will be kept on file:

- Application form
- References
- Record of training and support received, including supervision notes.

Staff and volunteers are responsible for ensuring that all records are kept confidential and secure. All records, both paper and electronic, are stored securely and processed in line with the organisations **Data Protection and Data Retention Policy** and the **Staff Procedures for Advocacy Case Management and Record Keeping**.

Access and Storage

- Volunteers, staff and service users have the right under the Data Protection Act to have access to information about them. Service users will be given support to understand any written information about them
- All confidential electronic records are held securely on the Speak Out database
- System access is security and password protected
- Paper records are securely locked in a filing cabinet in the office
- Where a staff member or volunteer is working from home, paper records held should be limited and held securely in a locked box or cabinet. Records should be returned to the office as promptly as possible.
- Desks are kept clear of confidential records when staff members leave their desk
- Computers and other devices used for work must be password protected and locked when away from the desk/ not in use.

Transport

- Emails are encrypted during transit. Outlook is protected by password.
- Staff must limit information transported in person and do so only when it is essential. Staff must be vigilant about confidential information at all times.

Retention

- Records will be retained in line with Speak Out's **Data Protection and Data Retention Policy**
- Service user records will be retained for three years after the partnership/project ends
- Staff and volunteer records will be retained for six years after leaving the organisation.

See **Appendix B** for further information on do's and don'ts of confidentiality

9. Confidentiality and the Speak Out Governance Board, Commissioners and Publicity

Board members and commissioners require feedback on the direction and performance of our projects; and their successes and failures. This will involve sharing anonymised information, including case studies/impact stories about our work with service users. All information given to Board members and commissioners about service users will be fully anonymised, and so consent from service users is not required.

In exceptional circumstances, an appointed Trustee of Speak Out will need more information about an individual. This will only occur in the case of a complaint, a safeguarding concern or where this confidentiality policy has been compromised.

To raise awareness about advocacy and/or the issues people with learning disabilities face, Speak Out may ask service users to 'share their story'. Case studies/impact stories can also help recruit new volunteers or to let other people know about Speak Out's work.

Before using a case study/impact story for wider publicity, that includes any identifying information, the service user(s) will be given full information on how their story will be used to help them decide if they are happy for their story to be shared. Written consent will then be obtained and recorded.

Case studies/impact stories will be fully anonymised (names, and other identify information changed, such as gender or other details), unless written consent to share personal information including their image is obtained from the service user.

10. Implementing these guidelines

The following action will be taken to ensure that these guidelines are effectively implemented:

- Confidentiality will be discussed as part of the induction of new volunteers and staff.
- This policy will be explained to people with learning disabilities who use our services at initial meetings, using Speak Out's accessible Confidentiality Policy, and a copy or summary of this policy will be made available to them.
- The Governance Board will regularly review this policy in line with Speak Out's Policy review schedule.

Appendix A: Categories of Confidential Data

Personal Data (taken from GDPR)
Personal data is any information that can cause a person to be identified, both directly and indirectly. This may be by identifiers such as: • a name; • an identification number; • a location; • an online identifier: • or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories Data (taken from GDPR)
Some of the personal data you process can be more sensitive in nature and therefore requires a higher level of protection. The UK GDPR refers to the processing of these data as 'special categories of personal data'. This means personal data about an individual's: • race; • ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data (where this is used for identification purposes); • health data; • sex life; or sexual orientation. • Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

Personal Confidential Data - Personal and Special Categories of Data owed a duty of confidentiality (under the common law).
This term describes personal information about a person which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'**.**

Appendix B:

Summary of Confidentiality Dos and Don'ts

Do

- Do protect the confidentiality of all personal information that you come into contact with.
- Do clear your desk at the end of each day, keeping all confidential records containing in filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to personal information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making
- A request for personal or confidential information and ensure they have a need to know.
- Do make clear to any third parties that any information shared with Speak Out staff about a service user will also be shared with the service user.
- Do share only the minimum information necessary.
- Do transfer confidential information securely by email using a Speak Out email account
- Do seek advice if you need to share personal information without the consent of the person and record the decision and any action taken
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and 'awareness raising' sessions on confidentiality issues.

Don't

- Don't share information without the consent of the person to which the information relates, unless there is a lawful reason to do so.
- Don't use personal information unless absolutely necessary and anonymise the information where possible
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary
- Don't share passwords or leave them lying around for others to see.