# GDPR, Data Protection, and Confidentiality Policy

Approved by Stand-by-Me Trustees: 29/5/20

Updated: 29/5/20
To be reviewed:29/5/21

**Stand-by-me Children's Bereavement Support Service**
**GDPR, Data Protection, and Confidentiality Policy**

## 1. General principles

1.1 Stand-by-me recognises that colleagues (employees, volunteers, trustees) gain information about individuals and organisations and service users during the course of their work or activities. In many cases such information will not be stated as confidential and colleagues must exercise common sense and discretion in identifying whether this information should be communicated to others. Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

1.2 Confidential information includes anything that contains the means to identify a person, e.g. name, address, post code, date of birth, National Insurance Number, passport and bank details. It includes information about sexual life, beliefs, commission or alleged commission of offences, clinical information and other sensitive personal information as defined by the Data Protection Act. It also includes information about organisations such as confidential business plans, financial information, contracts, trade secrets and procurement information

1.3 Colleagues should seek advice from their line manager about confidentiality and sharing information as necessary

1.4 Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual.

1.5 Where there is a statutory duty on Stand-by-me to disclose information, the person or people involved will usually be informed that disclosure has or will be made unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access.

1.6 Confidential information will be stored securely. It will not be left on desks but locked away. On computer it will be stored in securely encrypted folders.

## 2. Why information is held

2.1. Most information held by Stand-by-me relates to service users, individuals, voluntary and community organisations, self-help groups, volunteers, employees, trustees or services which support or fund them.

2.2. Information is kept in order to enable Stand-by-me colleagues to understand the history and clinical needs of service users as well as activities of individuals or organisations in order to deliver the most appropriate services.

2.3. Stand-by-me has a role in putting people in touch with voluntary and community organisations and keeps contact details which may be passed on to any enquirer, with the express consent of the individual.

2.4. Information about protected equality characteristics of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders. It is stored separately from any clinical records.

## 3. Access to information

3.1. Information regarding employees, volunteers, trustees and service users is confidential to Stand-by-me as an organisation and may be passed to colleagues, line managers or trustees on a need to know basis to ensure the best quality service for users.

3.2. Where information is sensitive, i.e. it involves personal or clinical information, disputes or legal issues, it will be confidential to the service user, or to the employee/Trustee dealing with the case and their line manager.

3.3. Colleagues will not withhold information from their line manager unless it is purely personal.

3.4. Users may have sight of Stand-by-me records held in their name or that of their organisation. The request must be in writing to the GDPR Officer and information will be supplied within 30 days in accordance with GDPR guidelines. Sensitive information as

outlined in para 3.2 will only be made available to the person or organisation named on the file.

3.5. Employees may have sight of their personnel records by giving 14 days' notice in writing to the Chair of Trustees.

3.6. When photocopying or working on confidential documents, colleagues should ensure people passing do not see them. This also applies to information on computer screens.

## 4. Storing information

4.1. General non-confidential information is kept in a locked office or locked filing cabinets and in computer files with open access to all Stand-by-me colleagues.

4.2. Personal information on employees, volunteers, trustees and other individuals working within Stand-by-me will be kept in lockable filing cabinets and will be accessible to authorised Staff and Clinical Trustees.

4.3. Clinical information is recorded and stored in a locked filing cabinet with restricted access until scanned to a secure computer file. Once scanned, any paper copies will be securely shredded.

4.4. Clinical information will only be held for as long as clinically necessary.

4.5. Employee records will be kept for 6 years following the end of employment.

4.6. Volunteer records will be kept for 2 years following the end of their volunteer tenure.

4.7. In an emergency situation, the Chair of Trustees may authorise access to files by other people.

## 5. Duty to disclose information

5.1. There is a legal duty to disclose some information including:

5.1.1. Child and vulnerable adult abuse will be reported to the relevant statutory services

5.1.2. Drug trafficking, money laundering or acts of terrorism will be disclosed to the police.

5.2. In addition, colleagues believing an illegal act has taken place, or that a service user is at risk of harming themselves or others, must report this to the Chair of Trustees who will report it to the appropriate authorities.

5.3. Users should be informed of this disclosure unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access

## 6. Disclosures

6.1 Stand-by-me complies fully with the DBS Code of practice (available from www.gov.uk) regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

6.2 Photocopies of DBS certificates will not be kept. However, Stand-by-me will keep a record of the date of issue of a Disclosure, the name of the subject, and the unique reference number of the Disclosure.

## 7. Data Protection Act

7.1. Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles. These are that personal data must be:

- Obtained and processed fairly and lawfully.

- Held only for specified lawful purposes.
- Adequate, relevant and not excessive.
- Accurate and where necessary kept up to date.
- Not kept longer than necessary, for the purpose(s) it is used
- Processed in accordance with the rights of the data subject under the Act.
- Appropriate technical and organisational measures are taken to guard against loss or destruction of, or damage to, personal data
- Not transferred to countries outside the European Economic Area without an adequate level of protection in place.

## 8. Breach of confidentiality

8.1. Misuse of personal data and security incidents must be reported to line managers so that steps can be taken to rectify the problem and ensure that the same problem does not occur again. This includes unauthorised access to person-identifiable information where a member of staff, or third party, does not have a need to know. It also includes incidents of information lying around in a public area, theft and loss of information.