Data Protection Policy

Purpose:

This policy sets out *[insert name of organisation]*'s approach to data protection together with responsibilities for implementing the policy and monitoring compliance. This policy is designed to meet all relevant legal requirements and to ensure that the reputation of *[insert name of organisation]* is not damaged through inappropriate or unauthorised access and sharing.

Responsibilities:

This policy applies to all staff, including senior managers and the board of trustees, paid staff, volunteers and sessional workers, agency staff, students or anyone working on behalf of *[insert name of organisation]*.

[insert name of organisation] trustees have overall responsibility for Data Protection within the organisation. Day-to-day responsibility for implementing and monitoring the data protection policy is delegated to *[insert name or role of person in the organisation]* including:

- understanding and communicating obligations
- reviewing the ways *[insert name of organisation]* holds, manages and uses personal information
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes
- monitoring and evaluating performance in relation to handling personal information

All *[insert name of organisation]* trustees and volunteers who process personal information must ensure they understand and act in line with this policy and the data protection principles. Breach of this policy will result in disciplinary action.

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. Staff and volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately.

Definitions:

Personal data is information that 'relates to' an 'identifiable individual' and is;

a) information processed, or intended to be processed, wholly or partly by automatic means (that is, information in electronic form usually on computer) or
b) information processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is usually paper records in a filing system)

This may include details of services users, as well as people who work for *[insert name of organisation]* as staff or volunteers, such as:

- Information on applicants for posts, including references
- Employee information – contact details, bank account number, payroll information, supervision and appraisal notes.
- Members – contact details
- Users – contact details (in many voluntary organisations, detailed case notes may be held)

Sensitive personal data includes:

- racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature

- trade union membership
- physical or mental health or condition
- sexual orientation
- criminal record
- proceedings for any offence committed or alleged to have been committed

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.

Data Subject - the individual whose personal information is being held or processed by [insert name of organisation] (for example: a service user or a volunteer)

Principles

[insert name of organisation] will:

- use personal information fairly and lawfully;
- collect only the information necessary for a specific purpose(s);
- ensure it is relevant, accurate and up to date;
- only hold as much personal data as we need, and only for as long as we need it;
- allow the subject of the information to see it on request; and
- keep it secure.

[insert name of organisation] will notify the Information Commissioners Office (ICO) about the data processing activities of *[insert name of organisation]* by registering with the Information Commissioner. The details are recorded on the public register and *[insert name of organisation]* renews this annually as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

[insert name of organisation] is transparent about how we intend to use data. We include privacy notices on our website and any forms that we use to collect data. These clearly explain the reasons for using the data, including any disclosures.

We avoid collecting data without a legitimate business reason and collect only the minimum required to meet the purposes we need it for and which are specified in our privacy notice.

We do not process personal data in any manner that is incompatible with the specified purposes. If we want to use personal data for a new or different reason that was not anticipated at the time of collection, we will consider whether this would be fair. Where needed, we will get consent to use or disclose personal data for a purpose that is additional to, or different from, the purpose we originally obtained it for.

The personal data we hold is accurate and, where necessary, kept up-to-date. Where we identify any inaccurate data, we update the records accordingly. We regularly review information to identify when we need to correct inaccurate records, remove irrelevant ones and update out-of-date ones.

We identify what types of records or data sets we hold and discard, delete or anonymise personal data as soon as it becomes surplus to requirements. We have a written retention policy which specifies when and how we will securely dispose of different categories of data.

We protect personal data using appropriate security measures. We assess the risks to the personal data we hold and choose security measures that are appropriate.

We do not transfer personal data outside the European Economic Area.

All staff handling personal data are briefed on their data protection responsibilities during their induction, with updates at regular intervals or when required. Specialist training will be provided for staff with specific duties such as marketing, information security and database management when necessary.

Transparency

[insert name of organisation] will be clear and open with individuals about how their information will be used. Individuals have a choice about whether they wish to enter into a relationship with *[insert name of organisation]* and if they know at the outset what their information will be used for, they will be able to make an informed decision.

When collecting data, *[insert name of organisation]* 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

Explicit informed consent is needed for processing sensitive data.

Subject access requests

We recognise and respond to any individuals' requests to access their personal data. The right of access gives anyone we hold personal data about the right to request, to see and obtain a copy of the information. We will respond to a subject access request promptly and in any event within 40 calendar days of receiving it.

- A subject access request should be made in writing. This includes email and by means of social media.
- *[insert name of organisation]* do not need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so provided that *[insert name of organisation]* are satisfied about the person's identity. If *[insert name of organisation]* considers a verbal request invalid, we will explain to the individual how to make a valid request.
- If a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, we will make a reasonable adjustment which may include treating a verbal request for information as though it were a valid subject access request.
- If a written request does not mention the Data Protection Act specifically or even say that it is a subject access request, it will be treated by *[insert name of organisation]* as valid.
- 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.
- 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 *[insert name of organisation]*. However if at any time we undertake the delivery of services under contract with the Local Authority we may be required to assist them to meet a Freedom of Information Act request where we hold information on their behalf.

Records management, retention and security

- 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.

- 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.
- *[insert name of organisation]* will routinely dispose of personal data that is no longer required, in line with agreed timescales (see Appendix)

Sharing data

[insert name of organisation] 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 *[insert name of organisation]* to disclose data (including sensitive data) without the data subject's consent. These are:

- carrying out a legal duty or as authorised by the Secretary of State
- protecting vital interests of a Data Subject or other person
- the Data Subject has already made the information public
- conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- 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.

[insert name of organisation] 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.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to *[insert name of organisation]* please contact *[insert name of person or role in organisation]*.

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