Sing Yourself Well

DATA PROTECTION POLICY AND PROCEDURES

Policy Statement

Sing Yourself Well recognises the importance of the correct and lawful treatment of personal data.

- Personal data is about living individuals that enables them to be identified such as name and address.
- Sensitive data refers specifically to data about race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

This policy explains how Sing Yourself Well handles data, what data is kept and why and how it ensures data remains safe and accurate. This applies to all personal data that we process regardless of the way that information is stored (e.g. on paper, electronically or by other means including email, minutes of meetings and photographs).

Glossary of Terms

- Senior Information Risk Owner – Trustee Level, responsible for setting policy (approving/adopting) and ensuring organisation compliant

- Data Controller – Decides what data is collected, what it is used for, how it is shared – in line with policy; 'instructs' data processors

- Data Processors – All staff who process data

- Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

- Data Subject/Service User – The individual whose personal information is being held or processed by Sing Yourself Well (for example: a volunteer, a client, an employee)

- 'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject to the processing of personal information about her/him. Explicit consent is needed for processing sensitive data

- Processing – means collecting, amending, handling, storing or disclosing personal information

- Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about

companies and agencies but applies to named persons or employees or individuals working for service user groups.

- Sensitive data – means data in areas:
    - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
    - trade-union membership;
    - genetic data, biometric data processed solely to identify a human being;
    - health-related data;
    - data concerning a person's sex life or sexual orientation.

Legal Requirements

The use of personal data is governed by the Data Protection Act 2018, the UK legislation that provides a framework for responsible behaviour by those using personal information. This is the UK's implementation of the General Data Protection Regulation (GDPR). The Information Commissioner's Office (ICO) is responsible for implementing and overseeing the Data Protection Act 2018.

- Sing Yourself Well is required to maintain certain personal data about individuals in order to carry out our work and legal obligations.
- Sing Yourself Well is the data controller for the information it collects and holds.
- Sing Yourself Well is currently not legally required to have a Data Protection Officer. However, a data protection lead has been identified and the person responsible for ensuring that Sing Yourself Well follows its data protection policy and complies with legislation is: Katy Baker & Abigail Pring.
- Sing Yourself Well *is not* required to register with the Information Commissioner's Office.

Aim and Scope of the Policy

The aim of this policy is to ensure that anyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures.
All those involved in Sing Yourself Well, who have access to personal information, will be expected to read and comply with this policy and training will be provided where necessary.

Individuals are personally responsible for processing and using personal information in accordance with the current legislation. Processing means collecting, amending, handling, storing or disclosing personal information.

Non-compliance or deliberate unauthorised disclosure of personal data may result in disciplinary action for staff/ termination of volunteering agreement. The trustees/directors are accountable for compliance of this policy and could be personally liable for a penalty arising from a breach they made.

This policy will be available for all volunteers, staff and Trustees and will be made available to relevant partners and stakeholders.

Principles of Data Protection

There are seven key principles of data protection. Compliance with the spirit of these principles is the foundation of good data protection practice. Sing Yourself Well fully endorses and adheres to these principles. Personal data we hold must be:

- Processed lawfully, fairly and in a transparent manner
- Collected only for legitimate purposes that have been clearly explained and not further processed in a way that is incompatible with these purposes (purpose limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
- Accurate and, where necessary kept up-to-date
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)
- Processed with integrity and confidentiality in a way that ensures appropriate security of the personal data
- Accountable, to those we hold data on and our stakeholders.

Data Collection

When collecting data, Sing Yourself Well will ensure that the individual:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should they decide not to accept
- Is, as far as reasonably practicable, competent enough to understand what processing would require
- Where necessary (for example, for special category data), grants explicit consent, either written or verbal for data to be processed
- Has received sufficient information on why their data is needed and how it will be used.

Data storage, retention and disposal

Information and records relating to individuals/members/service users will be stored securely and will only be accessible to authorised staff and volunteers. Information will be stored for only as long as it is needed or required by law and will be disposed of appropriately.

The retention schedule for data kept by Sing Yourself Well is as follows:

Data type	Location and security	Method of disposal and length of storage	Reason
Emails	*Securely in Sing Yourself Well Gmail account*	*deletion after 24 months*	*business need*
Mailing List	*Sing Yourself Well secure database*	*deletion if opted out and data cleansed every 4 years*	*business need*
Online surveys	*Database and SurveyMonkey*	*Deleted after analysis*	*business need*
Accident book	*In First Aid box in St Georges Extension*	*Shredding at 3 years from date of last entry (or, if involves child/ young adult, until they reach 21 years old) as per PCC guidelines*	*RIDDOR statutory regulation*
Trustee meeting Minutes	*electronically on password protected Sing Yourself Well Google drive*	*Kept for at least 10 years and deleted only when no longer required.*	*Legal compliance and business need*
Training and Event Registers	*secure database or paper sign-in sheets*	*Deleted from system after 12 months and paper shredded after 12 months*	*business need*

Data Accuracy

Sing Yourself Well will take reasonable steps to keep data accurate and up to date, such as:

- Only hold data where necessary to limit errors
- Discourage staff/volunteers from establishing unnecessary additional data sets
- Ask data subjects whether there have been any changes to their information
- Investigate and act upon notifications of inaccuracies
- Correct or delete data shown to be inaccurate
- Review and re-design the database system where necessary to encourage and facilitate the entry of accurate data

Data Security

Sing Yourself Well will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The measures taken include:

- Personal Data on paper will be kept in locked filing cabinets with access restricted to those who are authorised
- Password protection on personal information files
- Restricted access to computer files and systems
- Use of secure VPN mechanisms
- Data, including personal data, is backed up daily and information kept off site
- Encrypted attachments for sensitive personal information sent by email

It is Sing Yourself Well's responsibility to ensure all personal data is non-recoverable from a computer system passed on/sold to a third party that was previously used within the organisation. Any physical destruction of data will be undertaken in line with contractual obligations and any relevant British Standard.

I**ndividual Rights**

The GDPR provides the following rights for individuals:

- The right to be informed. Organisations processing personal information must provide fair information and be transparent over how they use personal data.
- The right of access. Individuals can request access to data held about them, known as Subject Access. The request can be made verbally or in writing, via any format including social media, to any Sing Yourself Well representative. The words 'subject access' are not needed for the request to be valid. Any such request should be reported to our Manager. Individuals can only access to their own data (or provide evidence they are legitimately acting on another person's behalf). Sing Yourself Well will respond to requests within one month. Information will be provided for free unless requests are overly excessive or repetitive, in which case an admin fee may be charged.
- The right to rectification. Personal data can be corrected if it is inaccurate or incomplete.
- The right to erasure. This right allows an individual to be 'forgotten' by requesting the deletion or removal of personal information where there is no compelling reason for its continued processing.
- The right to restrict processing. Individuals have a right to block or suppress the processing of personal data, for example if they contest its accuracy and are seeking verification, or where the organisation no longer needs the data, but the individual does, e.g. for a legal claim. The data can still be stored, but must not be used.
- The right to data portability. This gives individuals the right to obtain and reuse their personal data for their own purposes across different services. This only applies to data provided by the individual, based on consent or for performance of a contract and where processing is automated.
- The right to object. Individuals can object to direct marketing and processing. Sing Yourself Well gives all our service users choices about their marketing preferences when they first contact us and these preferences can be changed at any time.

Subject Access Request

Under the Data Protection Act 2018 individuals have the right to access data held about them as well as the right to be 'forgotten' where there is no longer a compelling reason to continue processing.

- A subject access request can be considered as any enquiry whether written (including email or webform) or verbal that asks for information you hold about the person

- Individuals can only request access to their own data (or must provide evidence that they are legitimately acting on another person's behalf). Sing Yourself Well may request proof of identity to ensure this.
- Sing Yourself Well may request further information on or clarification of the request.
- Information mentioning other people will be redacted if reasonable to do but may not be shared unless reasonable to do so or unless consent can be obtained for the relevant individual.
- Where requests are manifestly unfounded or excessive, in particular because they are repetitive, Sing Yourself Well may charge a fee or refuse to respond. However, individuals will receive a response to this affect and details of an appeals process (within the next calendar month).
- Sing Yourself Well will respond to any formal request within a calendar month. If there is a delay in obtaining the information requested then the request shall still be acknowledged within this period with an explanation for the delay and an expected date of response.

Members of the public may request certain information from statutory bodies under the Freedom of Information Act 2000. The Act does not apply directly to Sing Yourself Well. However, if at any time we undertake the delivery of services under contracts with relevant statutory bodies we may be required to assist them to meet the Freedom of Information Act request where we hold information on their behalf.

Disclosure and Data Sharing

Sing Yourself Well may need to share data with other agencies such as local authorities, funding bodies and other voluntary agencies as part of its work. The Data Subject will be made aware in most circumstances how and with whom their information will be shared as part of the Privacy Notice process.

However, there are circumstances where the law allows Sing Yourself Well to disclose data (including sensitive data) without the data subject's knowledge. These include:

- When required to by law – this may as simple as providing information to HMRC for tax purposes or if required by the police in relation to a crime.
- Protecting vital interests of a Data Subject or other person – this includes safeguarding concerns where an individual may be at risk or in cases of medical emergencies.
- The Data Subject has already made the information public.
- When conducting any legal proceedings, obtaining legal advice or defending any legal rights.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to individuals. Sing Yourself Well's data protection policy and procedures are designed to minimise the risks to individuals, and to ensure that the reputation of Sing Yourself Well is not damaged.

We make every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of how personal data incidents might occur include through loss or theft of data or equipment; ineffective access controls allowing unauthorised use; equipment failure; unauthorised disclosure (e.g. email sent to the incorrect recipient); human error; hacking attack.

In the event of a breach Sing Yourself Well will promptly assess the risk to individuals concerned and if appropriate report this breach to the ICO. If a report is required, Sing Yourself Well will notify the ICO as soon as possible, and not later than 72 hours after becoming aware of it.

Data Protection is everyone's responsibility. Staff and Volunteers are actively encouraged to report any incidents or concerns in order to improve both our data protection and services to users. If you know or suspect that a personal data breach has occurred, then you should immediately contact the Data Protection Lead, Katy Baker & Abigail Pring .

Policy agreed

4th April 2025
Signed KBaker
Signed APring

Review due April 2027