Scottish Working People's History Trust (SWPHT) Data Protection Policy

The Scottish Working People's History Trust needs to gather and use certain information about individuals that it has a relationship with or may need to contact. These individuals include trustees, volunteers and supporters, people who are contributing oral histories and reminiscence via recorded interviews, and other people the Trust works with.

The Trust also may collect and hold sensitive data relating to individuals via the collection of oral histories and reminiscence.

This policy describes how this personal and sensitive data will be collected, handled and stored to meet the Trust's data protection standards, and to comply with the UK Data Protection Act (2018) which replaces the 1998 Data Protection Act and encompasses the new General Data Protection Requirements-GDPR (2018).

This Data Protection Policy ensures the Trust:

- complies with data protection law and follows good practice
- protects the rights of volunteers, history interviewees and contributors, supporters and researchers
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach
- has clear processes in place in the event of a data breach.

Data Protect Act (1998) and General Data Protection Requirements (2018)

This legislation describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

It applies to all data that the Trust holds relating to identifiable individuals including names of individuals; postal addresses; email addresses; telephone numbers; bank details, age; gender; disability; ethnic background; political opinions; religious beliefs; trade union membership; health or sexual orientation.

The Data Protection Act (2018) is underpinned by important principles. These say that personal data must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Data Protection Risks

This Policy helps to protect the Trust from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the Trust uses data relating to them.
- Reputational damage. For instance, the Trust could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone operating on behalf of the Trust has some responsibility for ensuring data is collected, stored and handled appropriately. All trustees, volunteers and researchers with access to personal data must ensure that it is handled and processed in line with this Policy and data protection principles.

The Board of Trustees is ultimately responsible for ensuring that the Trust:

- meets its legal obligations with regard to data protection responsibilities, risks and issues
- reviews all data protection procedures and related policies
- arranges data protection training and advice for the people covered by this policy
- handles data protection questions from volunteers, oral history interviewees, researchers and anyone else covered by this policy
- ensures appropriate processes and systems are in place and adhered to to obtain specific and granular consent to hold individuals' personal and sensitive data, to record consent and to provide individuals with easy access to enable them to withdraw consent if they wish to do so
- deals with requests from individuals to see the data that the Trust holds about them
- checks and approves any contracts or agreements with third parties that may handle the Trust's sensitive data
- ensures all systems, services and equipment used for storing data meet acceptable security standards
- evaluates any third party services the Trust is considering using to store or process data
- approves any data protection statements attached to communications such as supporter leaflets.

General Guidelines

The Scottish Working People's History Trust will

- provide guidance to all trustees and volunteers to help them understand their responsibilities when handling data
- obtain specific and granular written consent by individuals taking part in oral history interview or recorded reminiscence activities
- obtain specific and granular written consent to publish and otherwise make publicly available information provided by individuals via oral history interview or reminiscence activities
- make it easy for individuals providing personal or sensitive data and information to withdraw consent for this information to be held by the Trust should they wish to do so, and will provide information on how to do this
- store recordings, and personal or sensitive data and information provided to the Trust securely
- ensure that the only people able to access data covered by this policy should be those who need it for their activities on behalf of the Trust
- Ensure that personal data is not disclosed to unauthorised people, either within the Trust or externally keeping data in as few places as necessary.

Trustees, researchers and volunteers will ensure all data is secure by taking sensible precautions and following the guidelines below:

- Review and update data regularly, and if it is found to be out of date or no longer required it should be deleted and disposed of.
- When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason. Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access. In particular, strong passwords must be used on devices used to store and access personal data, and these passwords should never be shared. Computers containing data should be protected by approved security software and a firewall.
- If data is stored on removable media (like a Digital Voice Recorder, CD or DVD), these should be kept securely when not being used.
- Data should be updated as inaccuracies are discovered. For instance, if a supporter can no longer be reached on their stored personal email or postal address, their details should be removed from the SWPHT database.

Personal data relating to Supporters of the Scottish Working People's History Trust obtained under Legitimate Interest will also be held securely following the above processes.

Data Breach

The Chair of the SWPHT should be notified if there is a suspected data breach. The Chair will instruct a team of Trustees to investigate the potential breach to establish if it is real, assess the impact on individuals and organisations and to resolve the breach. Individuals will be notified if there is a risk to their rights and freedoms, and, if appropriate, the Information Commissioner's Office will also be notified.

Access Requests and Privacy Statement

All individuals who are the subject of personal data held by **Scottish Working People's History Trust** are entitled to:

- ask what information the Trust holds about them and why
- ask how to gain access to it
- be informed how to keep it up to date
- be informed how the Trust is meeting its data protection obligations.

The Scottish Working People's History Trust aims to ensure that individuals are aware that their data is being processed, and that they understand:

- how the data is being used
- how to exercise their rights.

To these ends, the Trust has a Privacy Statement, setting out how data relating to individuals is used by the Trust. This is available on request and is also available on the SWPHT website.

Approved by the SWPHT Board of Trustees, 7th June 2022