Data Protection Policy					
Owner	Sam Best – Chief Operating Officer				
Date	12/07/2021	Version	6	CEO/Trustee Approved	12/07/2021
	12/07/2023		7		12/07/2023 MP

Statement of policy

SWEDA is fully committed to compliance with the requirements of the Data Protection Act. SWEDA will therefore follow procedures that aim to ensure that all employees, volunteers, and trustees who have access to any personal data held by or on behalf of SWEDA, are fully aware of and abide by their duties and responsibilities under the Act. This policy should be read in conjunction with SWEDA's GDPR policy.

To operate efficiently, SWEDA must collect and use information about people with whom it works. These may include members of the public, current, past, and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded, and used, (whether it be on paper, in computer records or recorded by any other means), and there are safeguards within the Act to ensure this.

SWEDA regards the lawful and correct treatment of personal information as very important to the success of its operations and the maintenance of confidence between us and those with whom we work. SWEDA will ensure that it treats personal information fairly, lawfully, and correctly.

To this end SWEDA fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018.

The principles of data protection

Everyone responsible for using data must follow strict rules called "General Data Protection Regulations - GDPR" They must make sure the information is:

1. Used fairly and lawfully
2. Used for limited, specifically stated purposes
3. Used in a way that is adequate, relevant, and not excessive accurate
4. Kept for no longer than is necessary
5. Handled according to people's data protection rights
6. Kept safe and secure (locked cabinets)
7. Not transferred outside of the building without adequate protection

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data
- That data and other information, which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Ethnic background
- Political opinions
- Religious beliefs
- Health
- Sexual health
- Criminal records

Handling of personal/sensitive information

SWEDA will through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, SWEDA will ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.

- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under an agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will follow approved procedures.

Data Security

All staff, volunteers, and trustees within SWEDA will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure and will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment and shredded when no longer required
- Handling methods will be reviewed every twelve months
- Personal data held on computers and computer systems is protected using secure passwords, which should be changed every three months
- Staff and Volunteers should avoid holding client records such as name and phone numbers on their personal phones, however if they need to store a client's telephone number on thier phone, they must ensure they use just the initials of the client. All text data should be deleted immediately.
- SWEDA's database which holds all client records will have 2 factor authentication passwords
- Individual passwords should be such that they are not easily compromised.
- Individuals accessing the SWEDA database from their work or personal pc's must ensure that they log out after each session and that passwords are always secure.
- Any data exported from the database for reporting purposes must be password protected or deleted immediately.
- Any client data emailed out should use initials or the client's individual client number on the database, never their full name.
- Staff/volunteers should be aware of what people can see during video calls and ensure confidentiality is always maintained.
- Staff/volunteers should avoid leaving laptops unattended and ensure time lapse password protection.
- If working from home staff/volunteer are encouraged to change the default password on their home router to reduce the chance of hacking.
- Staff/volunteers should avoid using public wifi hotspots, where no password is needed, as hackers can use these to set up bogus hotspots.
- Client data is only to be stored on the SWEDA secure database, not on desktops or USB drives.
- Any phishing emails should be forwarded to: report@phising.gov.uk
- SWEDA email addresses are set up via Office 365 and thus according to National Cyber Security Centre (NCSC) https://www.ncsc.gov.uk/collection/saas-security/product-evaluations/office-365 are secure to send personal data. However please be mindful when sending personal data that the forwarding email address is correct.

Implementation

The Chief Operating Officer will be responsible for ensuring that the policy is implemented and will also have overall responsibility for:

- The provision of data protection training, for staff, volunteers, and trustees within SWEDA, every 2 years.
- The development of best practice guidelines.
- Carrying out compliance checks with the Quality & Governance sub-committee to ensure GDPR adherence, throughout SWEDA, in line with the Data Protection Act.

Notification to the Information Commissioner

- The Information Commissioner maintains a public register of data controllers. SWEDA is registered as such.
- The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification through the IOC on an annual basis. Failure to do so is a criminal offence.
- The Chief Operating Officer will review the Data Protection Register with managers annually, prior to notification to the Information Commissioner.
- Any changes to the register must be notified to the Information Commissioner, within 28 days.

When information can be withheld

There are some situations when organisations are allowed to withhold information, for example if the information is about:

- The prevention, detection, or investigation of a crime
- National security or the armed forces
- The assessment or collection of tax
- Judicial or ministerial appointments

An organisation doesn't have to say why they're withholding information.

For further reference please refer to SWEDA's:

- GDPR Privacy Policy
- GDPR Data Audit
- Confidentiality Policy

THE COACH HOUSE • HARVEST COURT • SHEPTON MALLET BA4 5BS • 01749 343344 • WWW.SWEDAUK.ORG

UK Registered Charity 1056441; UK Company Limited By Guarantee 3208772