



C.1 DATA PROTECTION POLICY

This Policy is supported by documents:

- C.1 Data Protection Suite
- C.2 Communications Suite
- SG.1 General Safeguarding Suite
- SG.2 Child Protection Suite
- SG.3 Adults at Risk Suite

1. PURPOSE

South Wight Area Youth Partnership (SWAY) is committed to protecting the personal data of all individuals whose information we collect, use or hold, including children and young people, parents and guardians, staff, volunteers, trustees, donors and supporters.

This Policy sets out SWAY's approach to the responsible collection, use, storage, sharing and disposal of personal data and the measures we take to protect it.

SWAY will comply with applicable data protection legislation, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018; and
- relevant safeguarding and other legislation governing the handling and sharing of personal information.

The Trustees retain overall responsibility for ensuring that SWAY complies with its data protection obligations.

2. SCOPE

This Policy applies to everyone who works for, volunteers with, or acts on behalf of SWAY and who collects, accesses, uses, stores or otherwise processes personal data, including:

- Trustees
- Employees
- Volunteers
- Contractors
- Anyone processing personal data on behalf of SWAY

It applies to personal data held in **both digital and paper records**, regardless of where or how the information is stored.

Related Privacy Notices

This Data Protection Policy sets out how SWAY manages and protects personal data. It should be read alongside SWAY's Privacy Notices, which explain to individuals how their personal data is collected, used, stored and shared, and their rights in relation to that data.

SWAY maintains separate Privacy Notices for different groups, including:

- Children and young people and their parents or guardians
- Volunteers, staff and trustees
- Donors and supporters
- Website users

These Privacy Notices form part of SWAY's overall data protection framework and are reviewed regularly to ensure consistency with this policy.

3. ROLES AND RESPONSIBILITIES

Data Controller:

South Wight Area Youth Partnership (SWAY) is the Data Controller and determines the purposes and means of processing personal data.

Trustees

The Trustees retain overall accountability for ensuring that SWAY meets its data protection obligations and that appropriate policies, procedures and safeguards are in place.

Responsible Person / Data Protection Lead:

Manager: Steph Flux

The Data Protection Lead is responsible for overseeing SWAY's day-to-day data protection arrangements, providing guidance to staff and volunteers, maintaining appropriate records and procedures, and coordinating the response to data protection concerns and breaches.

Trustee with responsibility for Governance

The Trustee with responsibility for Governance provides Trustee-level oversight and support for SWAY's data protection arrangements.

Staff, volunteers, trustees and others processing personal data on behalf of SWAY must:

- comply with this Policy and relevant supporting procedures;
- only access and use personal data where authorised and necessary for their role;
- keep personal data secure and confidential;
- follow SWAY's requirements for storing, sharing and disposing of personal data; and
- report any actual or suspected data breach, loss, unauthorised access or disclosure immediately to the Data Protection Lead

4. DATA PROTECTION PRINCIPLES

SWAY processes personal data in accordance with the data protection principles set out in the UK GDPR.

Personal data must be:

1. **Lawful, fair and transparent** – processed lawfully, fairly and in a transparent manner.
2. **Purpose limited** – collected for specified, explicit and legitimate purposes and not used in ways that are incompatible with those purposes.
3. **Data minimised** – adequate, relevant and limited to what is necessary for the purpose.
4. **Accurate** – accurate and, where necessary, kept up to date.
5. **Stored only as long as necessary** – kept in a form which permits identification of individuals for no longer than necessary.
6. **Secure** – processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

SWAY also applies the accountability principle and maintains appropriate records, policies, procedures and other measures to demonstrate compliance with its data protection obligations.

5. TYPES OF PERSONAL DATA WE PROCESS

Depending on the nature of our work and the role or relationship of the individual, SWAY may collect and process different types of personal data, including:

Personal Data

- Name and preferred name
- Address and other contact details
- Date of birth
- Emergency contact details
- Attendance and participation records
- Photographs, video and other images
- Employment, volunteer or role-related information
- Equality, diversity and inclusion monitoring information

Special Category Data (where necessary)

Where necessary and lawful, SWAY may process special category data, including:

- Health or medical information
- Information relating to safeguarding
- Dietary information where it reveals information about an individual's health or beliefs
- Religious or philosophical beliefs, where relevant

Equality, Diversity and Inclusion (EDI) Information

Where necessary and lawful, SWAY may collect information relating to equality, diversity and inclusion for purposes including monitoring participation, understanding who benefits from our services, improving accessibility and inclusion, and meeting reporting requirements to funders and other relevant bodies. Some EDI information may constitute **special category data** and will only be collected and processed where an appropriate legal basis and any additional condition required by law apply.

Criminal Offence Data

Where legally required or otherwise permitted, SWAY may process information relating to criminal convictions and offences, including information obtained through DBS checks. Special category data and criminal offence data will only be processed where there is an appropriate legal basis and any additional conditions required by law are met. SWAY will apply appropriate safeguards to protect this information.

6. LAWFUL BASES FOR PROCESSING

SWAY will only collect and process personal data where there is a lawful basis for doing so under the UK GDPR. Depending on the purpose of the processing, SWAY may rely on one or more of the following lawful bases:

- **Consent** – an individual has given clear consent to the processing of their data for a specific purpose.
- **Contract** – processing is necessary to enter into or perform a contract, such as an employment or volunteer agreement.
- **Legal obligation** – processing is necessary for SWAY to comply with a legal requirement.
- **Legitimate interests** – processing is necessary for SWAY's legitimate interests, or those of a third party, provided that these interests are not overridden by the individual's rights and interests.
- **Vital interests** – processing is necessary to protect someone's life or physical safety and it is not possible to rely on another lawful basis.
- **Public task** – applicable where SWAY is carrying out a task in the public interest or exercising official authority.

SWAY will identify and document the appropriate lawful basis before processing personal data and will explain the relevant basis in its Privacy Notices where required.

Special Category Data

Where SWAY processes special category data, it will identify both:

- an appropriate **lawful basis** under Article 6 of the UK GDPR; and
- an applicable **condition for processing special category data** under Article 9 of the UK GDPR.

Depending on the circumstances, this may include explicit consent, obligations and rights in employment and social protection law, protection of vital interests, or substantial public interest, including where applicable provisions relating to safeguarding.

SWAY will apply appropriate safeguards when processing special category data.

SWAY will maintain a Record of Processing Activities (ROPA) to document its principal processing activities and demonstrate compliance with its data protection obligations.

7. CHILDREN AND YOUNG PEOPLE

SWAY works primarily with children and young people and recognises the importance of providing appropriate protection for their personal data. SWAY will:

- collect and process only data that is necessary and proportionate for the relevant purpose;
- provide appropriate privacy information to children and young people and, where appropriate, their parents or guardians;
- obtain parental or guardian consent where this is required for the particular processing activity;
- apply appropriate security measures to protect children's personal data;
- take particular care when processing sensitive or special category information relating to children and young people; and
- ensure that safeguarding responsibilities are taken into account when making decisions about the collection, use or sharing of personal information.

Children's personal data will not be used for marketing purposes unless there is an appropriate lawful basis and, where required, appropriate consent has been obtained.

8. TRANSPARENCY AND PRIVACY INFORMATION

SWAY will provide individuals with clear, accessible and appropriate information about how their personal data is collected and used. Privacy information will explain, where applicable:

- what personal data SWAY collects;
- why it is collected and how it is used;
- the lawful basis for processing;
- who the information may be shared with;
- how long the information is retained;
- individuals' rights in relation to their personal data; and
- how individuals can raise questions or concerns about the use of their information

This information is provided through SWAY's Privacy Notices, which are maintained separately as part of the C.1 Data Protection Suite.

SWAY will take reasonable steps to ensure that privacy information is provided at the appropriate time and in a form that is clear and understandable to the intended audience, including children and young people where appropriate.

9. DATA SHARING

SWAY will only share personal data where there is a lawful basis for doing so and the sharing is necessary and proportionate for the relevant purpose.

Personal data may be shared with appropriate organisations or individuals, including:

- emergency services, where necessary;
- safeguarding authorities and other relevant agencies where required or appropriate;
- HMRC and other regulatory or statutory bodies where required;
- banks and financial service providers where necessary to process payments;
- insurers, where necessary for insurance purposes or claims; and
- funders and commissioning bodies where necessary to meet agreed reporting or monitoring requirements and where the sharing is lawful

Before sharing personal data, SWAY will consider what information needs to be shared, who needs to receive it, the purpose of the sharing and whether appropriate safeguards are in place.

SWAY will not sell personal data.

Where safeguarding concerns arise, personal data may be shared without the individual's consent where there is a lawful basis for doing so and sharing is necessary to protect a child, young person or adult at risk, or to meet a legal or safeguarding obligation.

10. DATA RETENTION

SWAY will retain personal data only for as long as it is necessary for the purpose for which it was collected, or for as long as required by law or otherwise justified by a lawful and documented requirement.

SWAY will consider the purpose for which information is held, any legal or regulatory requirements, operational needs and the rights and interests of individuals when determining appropriate retention periods. Detailed retention periods for different categories of information are set out in SWAY's **C.2.k Record Retention** document.

SWAY will regularly review the information it holds and securely delete, destroy or anonymise personal data when it is no longer required, subject to any legal, safeguarding or other legitimate requirement to retain it.

Paper records containing personal data will be stored securely and securely destroyed when no longer required.

11. SECURITY MEASURES

SWAY will take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage or disclosure.

Depending on the nature and sensitivity of the information, security measures may include:

- password protection and appropriate access controls;
- secure cloud-based systems and devices;
- secure storage of paper records;
- restricted access to personal and sensitive information on a need-to-know basis;
- appropriate additional protection for DBS and other sensitive information;
- regular software and security updates;
- appropriate data back-up arrangements; and
- secure disposal of information when it is no longer required

Access to personal data will be limited to individuals who require it for legitimate SWAY purposes and who are appropriately authorised.

Detailed requirements for IT and information security are set out in the C.2.c IT Security Policy.

12. DATA SUBJECT RIGHTS

SWAY recognises the rights individuals have in relation to their personal data under the UK GDPR. Depending on the circumstances, individuals may have the right to:

- be informed about how their personal data is used;
- access their personal data;
- have inaccurate or incomplete personal data corrected;
- have their personal data erased;
- restrict the processing of their personal data;
- receive their personal data in a portable format;
- object to certain processing of their personal data; and
- have rights in relation to automated decision-making and profiling.

SWAY will respond to requests in accordance with data protection law. The normal time limit for responding to a data subject request is **one month**, although this may be extended where permitted by law.

Requests will be handled in accordance with SWAY's C.1.i Data Subject Rights Request Procedure.

Individuals who are dissatisfied with how SWAY has handled their request may raise their concerns with SWAY and may also complain to the **Information Commissioner's Office (ICO)**.

13. DATA BREACHES

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data.

All actual or suspected personal data breaches must be reported **immediately** to the Data Protection Lead.

SWAY will:

- assess the nature and potential impact of the breach;
- take appropriate steps to contain and minimise the impact of the breach;
- record the breach and actions taken;
- notify the Information Commissioner's Office (ICO) within **72 hours of becoming aware of a notifiable breach**, where required by law; and
- notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

All data breaches will be managed in accordance with SWAY's C.1.f Data Breaches Procedure, with records maintained using the relevant C.1.g Data Breach Reporting Form and C.1.h Data Breach Log.

14. TRAINING AND AWARENESS

SWAY will ensure that trustees, staff, volunteers and others who process personal data on behalf of SWAY receive appropriate information, guidance and training relevant to their roles and responsibilities.

Training and awareness will include, where appropriate:

- data protection principles and responsibilities;
- confidentiality and secure handling of information;
- safeguarding and appropriate information sharing;
- recognising and reporting actual or suspected data breaches; and
- any specific requirements relevant to the individual's role.

SWAY will provide additional or refresher training where appropriate, including where there are significant changes to legislation, SWAY's activities, systems or procedures, or where an incident indicates that further training is needed.

15. REVIEW OF POLICY

This Policy will be reviewed annually, or sooner where necessary, including if:

- relevant legislation or regulatory requirements change;
- ICO guidance or other relevant guidance changes;
- SWAY's activities, systems or methods of processing personal data change significantly;
- a serious or significant data breach or other data protection incident occurs; or
- a review identifies that changes are required to ensure the Policy remains effective and appropriate.

The Data Protection Lead will coordinate the review and make recommendations for any required changes. The Trustees are responsible for approving the Policy and ensuring that it remains appropriate for SWAY's activities and obligations.

Written: August 2026

Approved:

Review Due: