



Data Protection Policy

August 2023

1. Policy Statement

Everyday Sophie Hayes Foundation will receive, use, and store personal information about our volunteers, participants, partners, and colleagues. It is important that this information is handled lawfully and appropriately in line with the requirements of the [Data Protection Act 2018] and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

This policy does not form part of any employee's contract of employment and may be amended at any time.

The CEO is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the CEO or reported in line with the organisation's Whistleblowing Policy or Grievance Policy.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves the use of personal data. It includes obtaining, recording, or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical, or mental health condition, sexual orientation, or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. Data Protection Principles

Anyone processing personal data, must ensure that data is:

- Processed fairly, lawfully and in a transparent manner.

- Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
- Adequate, relevant, and limited to what is necessary for the intended purposes.
- Accurate, and where necessary, kept up to date.
- Kept in a form which permits identification for no longer than necessary for the intended purposes.
- Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- Not transferred to people or organisations situated in other countries without adequate protection and without firstly having advised the individual.

5. Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others):

- Whether the individual has given their consent (for example, in explicitly requesting to be added to our communications or joining our volunteer team)
- The processing is necessary for performing a contract with the individual (for example, delivering the Sophie Hayes Foundation Employability Programme and its activities.
- For compliance with a legal obligation (for example, if required for safeguarding purposes)
- For the legitimate shared interest of the charity and individual (for example, in the case of an active volunteer).

When sensitive personal data is being processed, additional conditions must be met as below:

Sensitive personal data includes the following types of data:

- Racial or ethnic origin
- Political opinions
- Religious and philosophical beliefs
- Trade union membership
- Health, sex life or sexual orientation
- Genetic and biometric data

For the Sophie Hayes Foundation, any data provided that identifies an individual as a survivor of human trafficking would count as sensitive personal data. Therefore, the following conditions apply to information provided by referral partners or directly by survivors of trafficking (participants) themselves.

- a) No sensitive personal data should be stored on the Sophie Hayes SharePoint. Sensitive personal data including the full name, date of birth and contact details of survivors of trafficking can only be stored a secure database.

- b) Any information stored in physical notebooks should use pseudonyms to ensure the identity of the individual is not compromised should the notebook be found using a decoy code.
- c) All sensitive personal data that has previously been stored on a personal laptop should be deleted to ensure the only information stored by Sophie Hayes Foundation is compliant with item 5a).
- d) Each referral partner is required to gain explicit consent to provide information for the Sophie Hayes Foundation the Employability Programme Referral Form.

6. Processing for Limited Purposes

In the course of our work, we may collect and process the personal data set out in the Schedule 1. This may include data we receive directly from a data subject (for example, by completing website forms or by corresponding with us by mail, phone, email, at events or otherwise) and data we receive from other sources (including, for example, referral partner forms for Employability Programme purposes).

We will only process personal data for the specific purposes set out in the Schedule 1 or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter

7. Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

- The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
- Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
- The types of third parties, if any, with which we will share or disclose that personal data.
- The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.
- How individuals can limit our use and disclosure of their personal data.
- Information about the period that their information will be stored or the criteria used to determine that period.
- Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
- Their right to object to processing and their right to data portability.
- Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
- The right to lodge a complaint with the Information Commissioner's Office.
- Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
- Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.

- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

This information will be explicitly shared with an individual through additional text on the 'Contact us' form on the website, on our Volunteer with Us invite and on any manual sign-up sheets (e.g., at events). A summary of this will also be added to a link on Sophie Hayes Foundation email footers.

This information will also be provided on our referral forms for the Employability Programme, to ensure compliance through our referral partners.

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month. For example, if we are provided the email address of a potential programme partner, volunteer or participant by a referral partner or another team member we must contact them within one month to confirm consent and engagement with us.

8. Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. This means the following approaches:

- That our referral forms will continue to only request information relevant for the delivery of the Employability Programme and other services.
- That we will only collect information needed explicitly for the relevant purpose from volunteers, partners, and potential donors.

9. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

This means that every staff member who processes data with Sophie Hayes Foundation has a duty of upkeep to changes in the data provided to them. This could be the accuracy of data regarding volunteers, participants, employees, referral partners or donors.

10. Timely Processing

We will not keep personal data for longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

In practice this means the following:

- **Volunteers:** If a volunteer has been inactive with us for a period of 1 year or chooses to 'Opt Out' from receiving updates, they must be deleted from all volunteer databases, email lists and email contacts.
- **Employability Programme Participants:** If a participant finishes Module 1 but does not want to engage with Module 2 or CREW and has not given explicit consent to be contacted in the future and we have not heard from them within 1 year of their referral to us, their details must be erased from all databases, email contacts and phones. They can be replaced with a pseudonym (e.g., Participant 1) for reporting purposes, but this must not store any personal data (e.g., age or contact details) alongside it. They can be provided with an info@sophiehayesfoundation.org contact email if they wish to re-contact us. The owner of the referral form and relevant spreadsheet needs to delete this data appropriately.
- **Module 2 Participants:** If a Module 2 participant finishes this module and has not given explicit consent to be invited to CREW events, then their details must be erased from all databases, email contacts and phones. They can be provided with an info@sophiehayesfoundation.org contact email if they wish to re-contact us.
- **CREW Participants:** All future CREW attendees must explicitly give consent at the end of Module 3 to be able to be contacted by Sophie Hayes Foundation. If a CREW participant has not attended for the period of 1 year, then they must be contacted with a request to re-confirm interest in receiving invites to attend CREW and the provision of info@sophiehayesfoundation.org contact email. If they do not respond within 3 months, then their details must be erased from all databases, email contacts and phones.
- **Referral Partners:** Referral partners are removed off email if no legitimate interest is present. All referral partners have the option to unsubscribe from contact emails through instructions in sender signature.
- **Donors:** Need to explicitly opt into additional contact from the charity, with an option to opt out
- **Supporters:** We only add people to newsletters when they have given explicit consent to do so.

11. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Confirmation as to whether or not personal data concerning the individual is being processed.
- Request access to any data held about them by a data controller (see also Clause 15 Subject Access Requests).
- Request rectification, erasure, or restriction on processing of their personal data.
- Lodge a complaint with a supervisory authority.
- Data portability.
- Object to processing including for direct marketing.
- Not be subject to automated decision-making including profiling in certain circumstances.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored, or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

For Sophie Hayes Foundation, this means that for any partners we refer to (for example, outreach partners, businesses, or charities), we need to have a signed agreement in place they will follow our data security principles.

We will maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorized to use the data can access it. SHF will administer this in three ways:
 - Only relevant staff will have access to personal data records kept by SHF
 - A monthly audit check on access to this folder
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on Sophie Hayes Foundation database (eTapestry) computer system (Microsoft) instead of individual PCs apart from sensitive personal data.

Security procedures include:

- Entry controls. Any unrecognized email access on the SharePoint site should be reported through email to the Data Protection Manager.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal sensitive data is always considered confidential). If lockable desk is not available, data should be secured in a locked folder or case.
- Data minimization. Sophie Hayes Foundation should only collect data as appropriate for the purpose as detailed in section 5.
- Pseudonymization and encryption of data: Every individual stored on work or personal phones should be encrypted with a pseudonym.
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- Equipment. Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. This includes SHF staff or volunteers ensuring they do not complete confidential databases when at risk of being seen by members of the public in public spaces.

- Avoiding Transferring Personal Data Outside of the EEA. Sophie Hayes Foundation will not pass on personal data to partners outside of the EEA. This includes personal data about colleagues, partners, or participants.

14. Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our organisation, Sophie Hayes Foundation as defined in the Charities Act (2016).

15. Subject Access Requests

Individuals must make a formal request for information we hold about them. Employees who receive a request should forward it to the CEO immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible.

16. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

If you have any questions, please send these to admin@sophiehayesfoundation.org, and for further information see the Information Commissioner's guidance here: <https://ico.org.uk/for-the-public/personal-informa...>