Data Protection Policy

Policy prepared by	Chris Baillie, Director
Date policy issued	June 2024
Date approved by Trustee Board	June 2024
Impact assessment completed	Yes
Policy review date	June 2026

Equality Impact Assessment Form

The completion of the Equality Impact Assessment (EIA) will help us to ensure that our policies, procedures and practices do not discriminate or disadvantage people and also improve or promote equality.

In relation to age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation.
Please explain if you identified any inequalities or possible discrimination in the policy, procedure or practice?
No negative impact on any of the equality strands identified in the procedure.
If identified, how have you changed the policy, procedure or practice to remove or mitigate the inequality or discrimination?
Not Applicable
Any follow up actions required?
Not Applicable

1. Introduction

Swarthmore is committed to protecting the rights and freedoms of individuals and safely and securely processing their data in accordance with all our legal obligations.

We hold personal data about our employees, trustees, volunteers, customers and suppliers and other individuals for a variety of business purposes.

The purpose of the policy is to set out how Swarthmore manages the collection, retention, use of and disposal of data, documents and other information.

Complying with this policy is important not only in order for the Swarthmore to meet its legal obligations, but also to ensure that everyone we hold data on; whether students, employees, trustees or volunteers, is treated fairly through the holding of that data, the way it is used and the manner in which it is disposed of.

2. Scope

This policy applies to all employees, trustees, volunteers, suppliers and customers of Swarthmore facilities. It applies to all areas of Swarthmore and covers documents and data that are held in both electronic and paper format.

3. Definitions

The key terms used in this policy are defined in the Glossary of Terms (Appendix A). These definitions are designed to be consistent with their use in the GDPR

Personal data held by Swarthmore principally concerns the following groups:

- Employees
- Volunteers
- Trustees
- Students
- Customers
- Suppliers

4. Principles

Personal data processed by Swarthmore will abide by the general principles set out in the GDPR. These principles are set out in Appendix B

No personal data will be made available to any third party unless a) there is a legal obligation to disclose it, most often this being a contractual requirement imposed by the funder; or b) the relevant data subject has given approval to disclosure or c) disclosure is considered to be in Swarthmore's legitimate interest, which is not outweighed by any potential prejudice to the affected data subject's interests. This means that we will not sell, or pass on, personal data purely for financial gain. However, we do use the personal data we hold to contact individuals with information about new courses or news about the centre and these do include requests to support Swarthmore in a number of ways, including financially. Where there is an on-going relationship with the data subject, for example with students, and they have been judged as to expect such communications, the Swarthmore will use the legitimate interest basis for this type of contact.

Any deliberate misuse of personal data may be considered to be a disciplinary offence and may be considered to be gross misconduct, depending upon the circumstances.

Under GDPR, Swarthmore is classified as the Data Controller and a Data Processor.

As a Data Controller we are accountable for the personal data we process. This means that for each type of personal data held we must be able to demonstrate that we comply with the requirements of the GDPR.

We must maintain our appropriate registration with the Information Commissioners Office (IOC) to continue lawfully controlling data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller.

5. Responsibilities

Trustees are responsible for:

- Ensuring that Swarthmore has a comprehensive policy on data and records management that, if properly implemented, will enable Swarthmore to meet all of its responsibilities in this area and will help support the achievement of its mission.

The Director is responsible for:

- Ensuring that the policy is updated in line with any changes of legislation or operational requirements.
- That the policy is reviewed every 3 years, and
- Where any major changes are proposed to way data is collected, held, analysed or disposed of, that an impact assessment is carried out, and
- That any breaches are reported to the Information Commissioners Office within the prescribed 72 hours.

The Management Team is responsible for ensuring:

- That the agreed policy is implemented across Swarthmore, and
- That appropriate training is made available to all employees at induction and at 3 yearly intervals, include general awareness raising for all employees and specific training for data owners.

All employees are responsible for:

- Fully understanding their data protection obligations.
- Checking that any data processing activities they are dealing with comply with our policy and are justified.
- Not using data in any unlawful way.
- Not storing data incorrectly, be careless with or otherwise cause us to breach data protection laws and our policies through their actions.
- Complying with this policy always.
- Ensuring that personal data about them, held by Swarthmore, is accurate and up to date.
- Raising any concerns, notifying any breaches or errors, reporting anything suspicious or contradictory to this policy or our legal obligations without delay to the Director or one of the Management Team.

6. Security

All personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Director will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Printed data will be shredded when it is no longer needed.

Data stored on a computer will be protected by strong passwords that are changed regularly. The use of memory sticks or CDs is discouraged, but where this is unavoidable these must be encrypted or password protected and locked away securely when they are not being used.

Personal data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

Servers containing personal data must be kept in a secure location, away from general office space and be protected by security software.

Paper records will be given the same level of security consideration as electronic records. Financial information, particularly where unauthorised access could give rise to a potential financial loss to the data subject, and sensitive personal data will only be kept in a locked environment.

All personal data and data key to Swarthmore's operations held in electronic form will be backed up on a regular basis. Any paper records adjudged to be critical will have electronic copies made.

7. Use of CCTV

Swarthmore uses CCTV for the purpose of the detection and prevention of crime. The use of CCTV and the legitimate purpose for its use, is widely advertised in the parts of the building where it is in use. The system is used overtly and there is no attempt to conceal its usage.

8. Meeting our obligations under the General Data Protection Regulations (2016)

Special categories of personal data

Previously known as sensitive personal data, special categories of personal data is data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law, for example to comply with legal obligations to ensure health and safety at work. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

In order to comply with the regulations, Swarthmore is required to identify the types of personal data that it holds and to show that, for each type, it has met its obligation namely:

- That it has determined the legal basis for processing the data (See Appendix D)
- That the DP principles (Appendix B) have been met
- That the individuals concerned have been properly informed (Appendix E)
- That the data is kept in an appropriately secure environment and
- That the data is being effectively managed so that it remains accurate and up to date and that it is disposed of when it is no longer required.

In addition to the management of the personal data it processes, the following sections address how Swarthmore meets these further requirements:

- The rights of individuals
- Subject Access Requests
- Dealing with data breaches

9. Rights of Individuals

Swarthmore is committed to ensuring that all employees understand their responsibilities as far as the rights of individuals are concerned.

Under GDPR there are a number of specific rights, outlined below, that may be relevant in dealing with individuals:

- The right to be informed
  Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language. Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency

- The right of access
  Requests to access personal data should be responded to as soon as possible and within one month at the latest (see section 7.4)

- The right to rectification
  As far as possible there should be a process in place that automatically updates any personal data that have been changed. Any data subject will have the right to request a change in any of their personal data if it is not correct.

- The right to erasure
  We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

- The right to restrict processing
  This right exists in specific circumstances. The right of the data subject will need to be weighed against the legitimate needs of the organisation.

- The right to object
  Individuals have the right to object to processing which is carried out for the legitimate purposes of Swarthmore or for direct marketing. In the case of the first Swarthmore can refuse if the needs of the organisation outweigh those of the individual. In the case of the second Swarthmore cannot refuse the request.

10. Privacy Notices

A privacy notice must be supplied at the time the data is obtained if obtained directly from the individual. If the data is not obtained directly from the individual, the privacy notice must be provided within reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children. See appendix E for detail of what must be included in a privacy notice.

11. Subject Access Requests

Access requests can be made by anyone for whom Swarthmore holds data.

Requests should be forwarded to the Director in writing. The Director will take reasonable steps to verify that the request has actually come from the data subject concerned.

The Director will seek to engage with the data subject as to the scope of the request if there is any doubt as to the actual data being requested.

Requests will be replied to within the statutory period of one month. Where possible the response time will be less than this. In exceptional cases the time limit can be extended by up to two months if it is a multiple and/or very complex request.

We can refuse to respond to certain requests and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission of the Director.

Under GDPR the individual is entitled to be given:

- A copy of all of the records held
- A description of the data held
- The reason(s) for the data being processed
- The origin of the data (if not provided by them)
- Who has been given the data or who may be given it and
- How long the data is expected to be kept

Any data subject who is not content with the accuracy or completeness of the response to their request for information has the right to appeal to the Chair of Trustees, within 10 working days of receipt of the response to their original request.

If the data subject is not satisfied with the response from the Chair of Trustees then they will be advised of their right to complain to the IOCs office.

Once a subject access request has been made, we cannot change or amend any of the data that has been requested. Doing so is a criminal offence.

External examination scripts are exempt from access requests.

12. Dealing with Data Breaches

What is a data breach?

A data breach is defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. There will be a breach whenever personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation, or if the data is made unavailable and that unavailability has negative effect on the individual. Examples of data breaches include, the loss of a USB stick, data being destroyed or sent to the wrong address, the theft of a laptop or hacking.

Seeing the data is sufficient to warrant the unauthorised access being defined as a breach. However, it is also likely to include the ability for someone to corrupt the data i.e. to amend or delete it and/or to copy it. In order to be a reportable breach, the unauthorised access only has to take place and there is no requirement for it to actually be used for any damaging purpose.

What data breaches should be reported?

Any data held by Swarthmore that is breached should be reported to the Director or another member of the Management Team, as soon as it is reasonably possible to do so. Preferably this should be done by email or alternatively by telephone.

All employees have a responsibility to report data breaches as soon as they become aware of them.
This allows us to investigate the failure and take remedial steps if necessary and maintain a register of compliance failures.

Any employee who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

The Director, other member of the Management Team, will report the breach to the ICO within 72 hours of being notified of it if the breach is judged to represent any risk to the rights and freedoms of the individuals. Any breach involving encrypted data does not need to be reported to the ICO. Any breach of unencrypted special data must be reported to the ICO regardless of the risk that it is considered to present to the rights and freedoms of the individuals.

During office hours the report will usually be one using the ICOs security breaches helpline (0303 123 1113)

Out of office hours the report will be made online using the ICOs security breach notification form click here for online form

Our response to a data breach

In the event of a data breach the Director, or other member of the Management Team, will:

- Undertake a risk assessment of the potential damage arising from the identified breach
- Notify the individuals concerned, as soon as reasonably possible, if there is considered to be a significant risk to their rights and freedoms, offering advice as to how the individual might protect themselves, where appropriate, and setting out how Swarthmore is responding.
- Take all reasonable steps to prevent the breach re-occurring
- Take all reasonable steps to recover and/or correct the data that has been breached

13. Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both the organisation and employees at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Director.