Swarthmore friendly learning	**Data Protection Policy**
Version:	Final
Author:	Joanna Stokes - Director
Date Issued:	June 2018
Date Approved by SMT:	
Impact Assessment Completed	Yes
Date of Next Review:	June 2021

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.

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

3. 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.

4. 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, 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
- Raise any concerns, notify any breaches or errors and report anything suspicious or contradictory to this policy or our legal obligations without delay to the Director or one of the Management Team.

5. 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.

6. 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.

7. 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

8. Rights of individuals

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

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

I. 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 u se personal data to demonstrate compliance with the need for accountability and transparency

II. 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)

III. 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 ot request a change in any of their personal data if it is not correct.

IV. 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.

V. 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.

VI. 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.

9. 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.

10. 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.

11. 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

12. Failure to comply

We take the 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.

Glossary of terms:

General Data Protection Regulations (referred to as GDPR)	The rules that update the original 1988 Data Protection legislation, effective 25 May 2018
Personal data	Any information that refers to an identifiable, living person that is held in a structured format
Special data	Particular personal data for example information about race or ethnicity (see Appendix C for full list)
Data subject	An individual to which the data refers
Data Controller/Owner	The person responsible for managing the data
Data Processor	A person or organisation responsible for processing data
Data Protection Officer	The person in the organisation who has the overall day to day responsibility for the management of personal data
Processing data	The organisation, adaption or alteration of data. The retrieval of, consultation with or use of data. The disclosure or dissemination of data. The alignment, combination and/or erasure of data
Privacy notice	The statement made by the Data Controller to the Data Subject explaining that their personal data is being held and all of the relevant information about this that they have the right to know
Subject Access Request	A request made by a Data Subject to be given copies of all of their personal data held and certain information about its use
Data Protection Impact Assessment	This is a risk assessment of the likely impact on personal data from any changes, such as changes to processes, adopting new technology or the introduction of a new activity
Data breach	When a security incident occurs that affects the confidentiality, integrity or availability of personal data
Data Protection by design	This is the commitment to always consider the impact on DP whenever a policy or process is amended

Appendix B

The Data Protection General Principles under GDPR

The following principles apply to the processing of all personal and special data:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(Note – the above is taken directly from the ICO website)

Appendix C

What is 'special' personal data?

Special personal data is personal data that refers to data in one, or more, of the following categories:

(a) Racial and/or ethnic origin;

(b) Political opinions;

(c) Religious or other beliefs of a similar nature;

(d) Membership of a trade union;

(e) Physical or mental health or condition;

(f) Sexual life;

(g) The commission of, or alleged commission of, any criminal offence; or

(h) Proceedings related to the commission, or alleged commission, of any criminal offence, the outcome of such proceedings or the sentence of any court in such proceedings

There are additional criteria that apply when considering the processing of special data (see Appendix D)

Appendix D

The legal basis for holding personal data

For each type of personal data held there must be one of the following legitimate legal basis for processing that data:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject (or to take steps to enter into a contract with the data subject)
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject (or another person)
- Processing is necessary to fulfil the legitimate purposes of the data controller (or a third party), except where such interests are overridden by the interests, rights or freedoms of the data subject

For each type of special personal data held there must be one of the following legitimate legal basis for processing that data:

- Explicit consent of the data subject (unless reliance is prohibited by law)
- Processing is necessary for carrying out obligations under employment, social security or social protection law or a collective agreement
- Processing is necessary to protect the vital interests of the data subject (or another) where the individual physically/legally cannot give consent
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim, providing that the processing relates only to members (or former members or those who have regular contact with it in connection with its purposes) and provided that there is no disclosure to a third party without consent
- Processing relates to data clearly made public by the data subject
- Processing is related to a legal claim or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest based in law which is proportionate to the aim pursued and which contain appropriate safeguards
- Processing is necessary of preventative or occupational medicine; for assessing the working capacity of an employee; medical diagnosis; the provision of health or social care treatment (or the management of lawful health or social care systems); or a contract with a health professional
- Processing is necessary for reasons of public health
- Processing is necessary for archiving in the public interest, or scientific and historical research or for statistical purposes (as defined by Article 89(1))

Appendix E

What we need to tell data subjects in our privacy notices

The requirements are set out in the table below:

Information to be supplied	When data obtained directly	When data obtained indirectly
Identity and contact details of the data controller and the DP Officer	✓	✓
Purpose of the processing and the lawful basis for it	✓	✓
The legitimate interests of the data controller	✓	✓
Categories of personal data	✓	✓
Recipients of personal data	✓	✓
Details of transfers to third countries and safeguards	✓	✓
Retention period or criteria used to determine retention	✓	✓
The existence of the data subject's rights	✓	✓
The right to withdraw consent at any time (where relevant)	✓	✓
The right to lodge a complaint with the ICO	✓	✓
The source of the data and whether the source was publically accessible	✓	✓
Whether the personal data is part of a statutory or contractual requirement and what the consequences of failing to provide the data might be	✓	
The existence of automated decision making processes	✓	✓

Appendix F

What we need to tell data subjects in our privacy notices

This table sets out minimum periods we will keep records (whether paper or electronic)

Type of Record	Minimum Retention Period	Other Information
Personnel files including documentation of grievance and disciplinary processes	6 years from the end of the individual's employment (Basic details – name, DOB and dates employed for 20 years)	Commitment to provide employment references and in case of litigation
Details of trustees	6 years after they cease to be trustees	
All information relating to redundancies involving less than 20 staff	6 years from the date of the redundancy	
All information relating to redundancies involving more than 20 staff	12 years from the date of the redundancy	
All records relating to maternity, paternity, adoption and parental leave pay	3 years from the end of the tax year they relate to	
Governance and constitutional documentation	12 years from any change in the documentation or from the point in time that the document is superseded	
Student records including academic achievement and performance	10 years (Basic details – name, DOB, courses attended and achievements for 20 years)	To be able to provide academic references
Student application forms	1 year	To be able to deal with any challenge from a student
All primary financial documentation including payroll information, invoices, signed accounts	6 years	Includes financial claims to the SFA

Type of Record	Minimum Retention Period	Other Information
Contracts	6 years from the end of the contract	
Returns to financial authorities (HMRC and pension providers)	3 years	
Returns to non-financial public bodies (such as the SFA)	3 years	
Property interests	12 years from the time of disposing of the property	Includes any secured loans or mortgages
Policies	6 years from the amendment of the policy or the point in time when it is superseded	
Application forms and selection process documentation	6 months	To be able to respond to any challenge to the recruitment/selection and appointment process
All documentation relating to accidents	3 years from the date of the last reported incident	
All Health & Safety compliance records	Until superseded by later records	
Reports from external bodies specifically regarding any aspect of the Settlement's activities	6 years (longer in specific instances)	This does not include reports of general interest that have not been compiled specifically about the Settlement
Health records (general)	During employment only	
Health records relating to the termination of employment	3 years	To be able to respond to any legal action
Governance documents including those outlining constitutional matters as well as minutes and resolutions	Permanently or 6 years after they have been superseded	

Note – the above minimums will be extended in the event of any specific requirements instituted by the approved authorities or where Swarthmore enters into any contractual arrangement where a longer retention period for documentation is specified.