GDPR/DATA PROTECTION POLICY

SWANMORE
COLLEGE

Centre of Excellence

Statutory	Yes
Website	No
Last Review	October 2024
Next Review	May 2025
Reviewer	Mr B Parker
Governor Committee	Resources
Ratified by BoG	November 2024

Contents

This policy sets out how the college deals with personal information correctly and securely and in accordance with the General Data Protection Regulation, and other related legislation.

1. Aims

Our college aims to ensure that all data collected about staff, pupils, parents, governors and visitors is collected, stored and processed in accordance with the Data Protection Act 1998. This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the provisions of the General Data Protection Regulation, which came into force in May 2018. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Sensitive personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed (Swanmore College)
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

Swanmore College collects processes and uses personal information relating to pupils, staff, governors and visitors, and, therefore, is a data controller. Swanmore College delegates the responsibility of data controller to the Headteacher.

Swanmore College is registered as a data controller with the Information Commissioner's Office and renews this registration annually. This information is gathered in order to enable the provision of education and other associated functions. In addition, Swanmore College may be required by law to collect, use and share certain information.

5. Data protection principles

The UK GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the college aims to comply with these principles.

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that the college complies with its obligations under the Data Protection Act 1998 and GDPR 2018.
Day-to-day responsibilities rest with the Headteacher and Data Protection Officer. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data. The College has also appointed a Data Protection Specialist, Dr P Sleat. Both the Data Protection Officer and the Data Protection Specialist have undertaken advanced iHasco training in GDPR.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the college of any changes to their personal data, such as a change of address, telephone number, and email contact.

College's Commitment

The college is committed to maintaining the principles and duties in the GDPR at all times. Therefore the college will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer.
- Inform individuals of the purposes that personal information is being collected and the basis for this.
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the college plans to transfer personal data outside the UK the college will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent *(where relevant)* and that if consent is withdrawn that the college will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept.
- Should the college decide to use an individual's personal data for a different reason to that for which it was originally collected the college shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium *(paper or electronic)* it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (*known as Subject Access Requests.*)
- Ensure that personal information is not transferred outside the UK without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

7. Privacy notices (Full copies are available on the GDPR section of college website)

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the college is performing. We may also receive data about pupils from other organisations including, but not limited to, other colleges, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests (Exams)
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy. We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our college. The purpose of processing this data is to assist in the running of the college, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the College Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the college holds should contact the Headteacher or Data Protection Officer.

8. Subject access requests (Request forms are available on GDPR section of college website)

Right of access

At a glance

Individuals have the right to access their personal data. This is commonly referred to as subject access. Individuals can make a subject access request verbally or in writing. You have one month to respond to a request. A fee cannot be charged to deal with a request in most circumstances.

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

Complying with subject access requests

We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.

.

What is an individual entitled to?

Individuals have the right to obtain the following from the college:

Confirmation that you are processing their personal data;
A copy of their personal data; and other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). If a subject access request is made digitally, the information must be returned in a digital format. If the request is made on paper, it should be returned as per the request. If this is not noted in the request, clarification should be sought before any information is provided.

Other information

In addition to a copy of their personal data, you also have to provide individuals with the following information:
the purposes of your processing; the categories of personal data concerned; the

recipients or categories of recipient you disclose the personal data to; your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it; the existence of their right to request rectification,

erasure or restriction or to object to such processing; the right to lodge a complaint with the ICO or another supervisory authority; information about the source of the data, where it was not obtained directly from the individual; the existence of automated decision-making (including profiling); and the safeguards you provide if you transfer personal data to a third country or international organisation.

The college will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be provided within a calendar month.

9. Parental requests to see the educational record (Request forms available on GDPR section of college website)

Parents have the right of access to their child's educational record, free of charge, within 15 working days of a request. Access to education records is a separate right and is not covered by Data Protection legislation. Unlike the right to access under Data Protection legislation, this right does not extend to pupils. Any information sought outside of the Education record request is subject to GDPR regulations. Any pupil above the age of 13 must give their consent before the information may be passed on to parents / guardians. This information must be provided within 30 days, unless an extension is granted.

10. Storage of records

Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept secure when not in use.

Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

Where personal information needs to be taken off site (in paper or electronic form), this will be carried out in accordance with the college's data mapping document.

Passwords that are at least 8 characters long containing letters and numbers are used to access college computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.

Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for college-owned equipment.

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records. Please refer to HCC Retention Schedule.

12. Training

Our staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation or the college's processes make it necessary.

13. The General Data Protection Regulation

The General Data Protection Regulation came into force in May 2018 as the law, updating the rights of data subjects. With this new legislation the college has worked to implement enhanced working practices, which has included clear desk policies, along with annual training on the GDPR via online training.

14. Monitoring arrangements

The Headteacher, Data Protection Officer and nominated governor representative are responsible for monitoring and reviewing this policy. This document will be reviewed annually. At every review, the policy will be shared with the full governing body.

15. Links with other policies

This general data protection policy and privacy notices is linked to the freedom of information publication scheme.

16. Personal data breaches

The college will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in

Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a college context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils
- Use of pupil's names in media/marketing without appropriate consent

Appendix 2.

All data breaches must be reported the Brett Parker (DPO / Business and Operations manager) or Dr P Sleat (Data protection specialist / Assistant Headteacher) within 24 hours of the breach being identified. This enables the breach to be reported to the ICO within the 72 hour timescale. A record of all self-referrals will be kept and maintained by them.

17.Complaints

Complaints will be dealt with in accordance with the college's complaints policy. Complaints relating to the handling of personal information may be referred to the

Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

18.Contacts

If you have any enquires in relation to this policy, please contact (Brett Parker Business and Operations Manager/Data Protection Officer) or in their absence, Dr P Sleat (Data Protection Specialist) They can be contacted via enquiries@swanmore-sec.hants.sch.uk.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

➢ Lost
➢ Stolen
➢ Destroyed
➢ Altered
➢ Disclosed or made available where it should not have been
➢ Made available to unauthorised people

- The DPO will alert the Headteacher and the Chair of Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen, following the ICO toolkit.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

➢ Loss of control over their data
➢ Discrimination
➢ Identify theft or fraud
➢ Financial loss
➢ Unauthorised reversal of pseudonymisation (for example, key-coding)
➢ Damage to reputation
➢ Loss of confidentiality
➢ Any other significant economic or social disadvantage to the individual(s) concerned If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a Data Log which saved on our internal network.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the colleges computer system.

The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions (some examples set out below) to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Example - Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as

they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO (or a member of SLT if parties are known by the DPO) will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- Any sensitive information sent out by the College will be password protected and have a 15 minute delay set for external emails.
- Any sensitive documents on CPOMS will only be viewed and not downloaded.
- All staff training will be given annually and in person.