SPARSHOLT COLLEGE GROUP

SPARSHOLT CAMPUS

ANDOVER CAMPUS

UNIVERSITY CENTRE SPARSHOLT

Data Protection Policy

Our Mission

Raising Aspirations, Unlocking Potential, Advancing Futures

Our Values

Excellence, Passion, Teamwork, Integrity, Innovation,

Sustainability, Valuing Others and Supportiveness

Sparsholt College Group

The Sparsholt College Group (the College Group) includes Sparsholt College, Andover College, University Centre Sparsholt, Sparsholt College Services, Westley Enterprises and Andover Town Football Club. College Group policies apply to each part of the group unless specified otherwise

The *Data Protection Policy* was approved by the Board of Governors in March 2026.

Next scheduled review: March 2029.

DATA PROTECTION POLICY

Contents

DATA PROTECTION POLICY

1. Introduction

Sparsholt College Hampshire ("the College") is registered as a Data Controller under the Data Protection Act 2018. The College is considered a public authority under the Freedom of Information Act 2000. Registration is renewed annually.

Data Protection Register
Registration Number Z6812070
Data Controller: SPARSHOLT COLLEGE HAMPSHIRE
Address:
SPARSHOLT
WINCHESTER
HAMPSHIRE
SO21 2NF

Further details regarding the registration are available via ico.org.uk

The College needs to keep certain information about employees, learners and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act 2018.

This policy, and references to 'the College', apply to all parts of the Sparsholt College Group.

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

2. The Types of Information Covered by Data Protection Legislation

Personal Data

Data Protection legislation applies to personal data relating to a living person. It applies not only to computerised or automated personal data, but also to information held in manual filing systems. Included are such items of information as name, date of birth, contact details, title and gender, but also less obviously personal data such as IP addresses, online identifiers and pseudonyms.
The legislation also applies to any records where an individual can be directly or indirectly identified from the information present, even where the name is not included. Throughout this document, "personal data" means all information and data relating to an individual.

Sensitive Personal Data

Also known as Special Category Data, this is the subset of Personal Data where the data items are especially sensitive and need a greater level of protection. These include ethnic origin, health data, religion, sexual orientation, and biometric information.

3. The College's Responsibilities

Under the Data Protection Act and the GDPR, the data protection principles set out the main responsibilities for the College. These require that data shall be:

a) processed lawfully, fairly and in a transparent manner
b) collected for specified, explicit and legitimate purposes and processed in an appropriate way
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
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
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing

The College must have a lawful basis for processing any personal data and must make this clear in the privacy notice.

"Personal data" means recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you. "Processing" means doing anything with the data, such as storing, accessing, disclosing, destroying or using the data in any way.

4. The Data Controller and the Designated Data Officers

The College as a body corporate is the Data Controller under the Act and the Board of Governors is therefore ultimately responsible for compliance with the statutory legislative requirements. The Principal takes this overall responsibility for compliance and delegates the overseeing of the implementation, giving advice and dealing with the subject access requests to the Data Protection Officer. There are also designated Data Officers throughout the College who deal with data on a day-to-day basis relating primarily to learner data and staff data matters.

The majority of subject access requests will be dealt with through individual Data Officers.

The MIS Manager, Head of Student Support and Student Administration Manager are Data Officers for data issues relating to the learners.

The Director of Human Resources is the Data Officer for all data issues relating to staff.

The Director of Information and Funding is the Data Protection Officer.

5. Fair and Lawful Processing

We will usually only process your personal data where the processing is necessary to comply with our legal obligations, for the protection of your vital interests, for our legitimate interests or the legitimate interests of others. The full list of conditions is set out in the GDPR.

Data processing may be legitimately carried out by third parties where appropriate. This is only done where the College has established a controller - processor agreement with suitable safeguards.

We will only process "special categories of data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, genetic data and data about sexual orientation where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the GDPR.

6. How We Are Likely to Use Your Personal Data

We will process data about staff for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits in connection with your employment.

We may process special categories of data relating to staff including, as appropriate:

(a) information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work.
(b) the employee's gender, sexual orientation, racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation.
(c) in order to comply with legal requirements and obligations to third parties.

7. Processing for Limited Purposes

The College will only process your personal data for the specific purpose or purposes notified to the individual or for any other purposes specifically permitted by the GDPR.

8. Adequate, Relevant and Non-Excessive Processing

Individuals' personal data will only be processed to the extent that it is necessary for the specific purposes notified to them.

9. Accurate Data

The College will keep the personal data it stores about individuals accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify the College if any personal details change or if someone becomes aware of any inaccuracies in the personal data the College holds about them.

10. Data Retention

The College will not keep individuals' personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from its systems when it is no longer required. The College's Information Retention Schedule sets out the number of years data will be retained for each category of data with which we work. The Retention Schedule is reviewed and approved by the Strategic Leadership Team (SLT).

11. The Rights of Individuals Whose Data is Processed by the College

a. The right to be informed
The College is obliged to provide fair processing information and does so through its privacy notices.

b. The right of access
Individuals have the right to access their personal data, and this access will be provided as quickly as possible – we are legally bound to provide the data within one calendar month. This data will usually be provided free of charge, with the only exception being where the request is found to be unfounded, excessive or repetitive. See Section 11 for details on how to access data.

c. The right to rectification
Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

d. The right to erasure
An individual is entitled to request the deletion or removal of personal data where there is no compelling reason for its continued processing. It should be noted that the College is legally obliged to process and retain much of the personal data it holds.

e. The right to restrict processing
Individuals have the right to restrict the College from processing certain aspects of their personal data if one of the following circumstances applies:

- The accuracy of the data is contested
- The individual objects to the processing of the data in principle
- The College's processing of the data is unlawful
- The College wishes to delete the data, but the individual has need of the data for legal purposes

f. The right to data portability
Individuals may request an electronic copy of their personal data to use for their own purposes. The College will make every effort to provide the data in a form that is useable and acceptable to the individual, and this will be done without charge.

g. The right to object
Individuals have the right to object to:

- Direct marketing – the College will stop processing for this purpose on receipt of an objection.
- Data processing for research or statistics – the College will engage with the individual to come to an agreement within the law.

- Data processing in the College's legitimate interests - the College will engage with the individual to come to an agreement within the law.

h. Rights in relation to automated decision making and profiling
Individuals who have any concerns about automated or computerised decision making should refer them to the Data Controller.

12. Automated Decision Making

The College uses software and AI agents to make recommendations rather than decisions, and decisions will not be made on such recommendations without human intervention/validation.

Users of the College IT services must remember that personal data fed into public Large Language Models (such as ChatGPT, Claude) may be put into the public domain, and that this may constitute a data breach.

CoPilot simplifies many administrative processes, but it should be remembered that in order to do so, it stores data. If this data includes personal data, it then can form part of the electronic record for that data subject and may be disclosed to them by request.

13. Responsibilities of Staff

- To ensure that the information provided to the College in connection with their employment, is accurate and up to date.
- To update the College of any change to information which they have provided.
- To check the information that the college will send out from time to time, (giving details of information kept and processed about staff), and advise of any information that is incorrect or incomplete.
- To comply with the guidelines for data collection and processing when, as part of their responsibilities, they collect information about other people (for example learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances).
- To not feed personal data into public Large Language Models (such as ChatGPT, Claude). Any such information is put into the public domain, and that this may constitute a data breach.
- Undertake a Data Protection Impact Assessment (DPIA) in conjunction with the College DPO, for any project work involving the use of AI prior to the commencement of the project. Should the project risk using data outside of college consents or risk exposing personal data to an external large language model, the DPO will refuse consent and refer the matter to a Senior Post Holder to consider whether the vetoed ambitions of the project can be realised without the potential to compromise personal data.

14. Responsibilities of Learners

- To ensure that all personal data provided to the College is accurate and up-to-date.

- To ensure that changes of address, next of kin etc. are notified to the College, preferably via the Learner Portal, but alternatively via Student Admin and/or any member of their Course Team.
- To ensure that they keep their passwords to College networks and systems secret and secure.
- To report to the College's IT Services team if they suspect their account security has been breached.

15. Data Security

The College will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The College has procedures and technologies in place to maintain the security of all personal data from the point of collection to the point of destruction. The College will only transfer personal data to a third party if that party agrees to comply with those procedures and policies, or if that party puts in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

In order to ensure the security of personal data, IT Services will:

- maintain a high level of security guarding the College's network and systems as detailed in the College's IT Policy
- enforce a minimum of 128-bit encryption on portable devices
- prevent users from storing data on local drives of non-portable IT hardware
- require a change of network password for staff every 90 days
- wipe hard drives and memory of all equipment before disposal

In order to ensure the security of personal data, staff are required to:

- lock their IT device using  **-L** when leaving their device unattended.
- keep their passwords secret.
- avoid opening emails on a projected screen – private information may be displayed to anyone else in the room or even outside via the window.
- when emailing personal data, password protect in an attachment and phone the password through to a trusted number.
- refer all requests for disclosure of personal data from external sources to be dealt with via the central register.
- only use College approved cloud based repositories (OneDrive for Business and SharePoint Online, accessed via their College email address).
- check the email addresses of intended recipients before sending any email, as email programs often incorrectly predict email addresses you are typing in.
- consider using BCC to restrict visibility of other recipients' addresses when emailing to a group of recipients (especially where there are large numbers of recipients or some external addresses).

- avoid copying any personal data into Large Language Model AI agents.
- remember when using the CoPilot transcription service that any references to individuals will be on the record and therefore disclosable.
- contact the Data Protection Officer (the Director of Information and Funding) if in doubt about any data security matter.

Where the College processes data on behalf of other organisations, e.g. conducting external DBS checks, it will comply with ICO requirements.

16. Breaches of Data Protection Principles

If an individual considers that the data protection principles have not been followed in respect of personal data about themselves or others, they should raise the matter with their line manager (members of staff) or a member of College staff (non-staff members).

The matter can alternatively be raised by emailing data.protection@sparsholt.ac.uk. Any breach of the GDPR will be taken seriously and may result in disciplinary action.

17. Loss or Theft of Personal Data

All incidences of loss or theft of personal data must be reported immediately to the College's Data Controller (the Director of Information and Funding). A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords, to the loss or theft of personal data either inside or outside the College.

A security incident is any event that has resulted or could result in:

- The disclosure of personal/sensitive/confidential data to any unauthorised person.
- The integrity of the system or data being put at risk.
- Threat to personal safety or privacy.
- Legal obligation or penalty.

All incidents must be reported to the Data Controller in the first instance, as soon as possible after the event.

In the case of a potential breach, the Potential Data Breach Procedure (Appendix A) will be followed. The Data Controller will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies, in particular the Information Commissioner's Office (ICO). If a breach has occurred, the ICO will be informed within 72 hours of the incident, and if appropriate all data subjects concerned will also be contacted and informed. If possible, the offending paperwork, data or communication will be retrieved as soon as possible. The Data Controller retains a central register of all such incidents occurring within the College, whether or not they resulted in a breach.

The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, you should consult the Data Controller who will decide what action should be taken.

Examples of a breach of confidentiality:

- Finding confidential/personal data either in hard copy or on a portable media device outside College premises or in any of the College's unsecured common areas.
- Finding any records about a staff member, student, or applicant in any location outside the College's premises.
- Passing information to unauthorised people either verbally, in writing or electronically.
- Unauthorised individuals gaining access to the College's IT systems, particularly the Student Records systems (ProSolution / ProMonitor) or the Human Resources system (Chris21).

18. Subject Consent

In many cases, the College can only process personal data with the consent of the Individual. In some cases, if the data is sensitive, express consent must be obtained.

Agreement to the College processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous unspent criminal convictions (all convictions in the case of staff).

Therefore, all prospective staff and learners will be asked to sign a Consent to Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

19. Requesting Access to Personal Data

In order to request access to your personal data (commonly known as a Subject Access Request), as held by the College, it is preferable that you submit a request by email to the Data Protection Officer (data.protection@sparsholt.ac.uk). However, requests can be made to any member of staff, electronically, in writing or verbally, on the basis that they will be passed to the Data Protection Officer.

The College undertakes to respond as quickly as possible to subject access requests within one calendar month of receipt of the request (the statutory maximum time allowed). Data disclosures will be undertaken free of charge in almost every case (repeat requests may possibly incur a charge at the discretion of the College).

20. Accountability

The Data Protection Officer will produce an annual report on data protection activities for presentation to the College's Senior Leadership Team and Board. This report will include detail of the following:

- Data Protection Disclosure Requests (Subject Access Requests)
- Data breaches
- Data breach near misses
- External organisations' breaches affecting staff and/or students
- Requests to be forgotten
- Staff data protection training

21. Conclusion

Compliance with the Data Protection Act 2018 is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of the policy should be taken up with the Data Protection Officer.

If you require any further information on the Data Protection Act 2018, or how any aspect of it is implemented at Sparsholt College, please make contact with:

Data Protection Officer
Sparsholt College
Winchester SO21 2NF
Tel: 01962 673288
Email: data.protection@sparsholt.ac.uk or foi@sparsholt.ac.uk

Related Policy:

Freedom of Information Publication Scheme

Useful Links:

Information Commissioner: www.ico.gov.uk
ICO GDPR Resources: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
JISC GDPR Resources: https://www.jisc.ac.uk/gdpr

Appendix A – Data Breach Procedures

Introduction

The Information Commissioner's Office (ICO) describes a data breach as follows: "A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes."

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any 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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.

These circumstances could come about either unintentionally, in ignorance of the law, or by deliberate breaking of the law.

A notifiable data breach must be reported to the ICO without delay, and not later than 72 hours after the College becomes aware of it.

Procedure

In the event that a data breach is suspected, the College's Data Protection Officer (DPO) must be informed immediately. In the absence of the DPO, the Chief Operating Officer & Deputy CEO should be informed, and a decision will then be taken about the conduct of the investigation.

The DPO is Scott Hermiston, Director of Information and Funding. His office is in the Admin Building at Sparsholt on the Finance corridor (F22). His contact details are as follows:

Telephone: 01962 673288

Email: scott.hermiston@sparsholtservices.ac.uk

or Data.protection@sparsholt.ac.uk

The first action of the DPO will be to take any measures available to contain the suspected breach, and also to identify the data subjects whose information may have been breached.

The DPO will launch an investigation into the circumstances of the suspected data breach and will make a decision about how to proceed within 24 hours. An assessment of the risks

posed by the nature of the data concerned to the data subjects will be made, and this will inform whether or not the individuals need to be contacted and if so, with what level of urgency.

In the event that the DPO forms the opinion that the event does not constitute a personal data breach, the investigation will be written up and retained in the Data Protection SharePoint online pages. The documentation will include a clear statement of the reasoning behind the decision not to treat the event as a personal data breach.

In the event that the DPO forms the opinion that the event constitutes a personal data breach, the DPO will communicate this to the College's Senior Leadership Team via the Chief Operating Officer & Deputy CEO.

If the breach involves "a high risk to the rights and freedoms of the individuals", then contact details will be compiled for all data subjects whose data was included in the breach, and a plan constructed for communicating the situation to them. The communication will include:

- the name and contact details of the Data Protection Officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed, to deal with the personal data breach
- a description of any measures taken to mitigate any possible adverse effects

The DPO will also compile a script for a telephone call to the ICO, which will include:

- what has happened
- when and how the College found out about the breach
- the people that have been or may be affected by the breach
- what we are doing as a result of the breach
- the contact details of the Data Protection Officer

The ICO can be informed in the following ways:

- By telephone on 0303 123 1113
- Using the online template, available at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Conclusion

Once all of the mandatory steps have been taken, the DPO will conclude the investigation by completing the report and publishing it to the College's Strategic Leadership Team. The report will detail the nature of the breach, its effects and the remedial action taken. The report will also address whether or not the breach was a result of human error or a systemic issue, and how a recurrence could be prevented – whether this is through better processes, further training or other corrective steps.

Flow chart for the response to a possible breach of personal data