

# Data Protection Policy

## *Integrity*



### **Our Mission**

To inspire learners to recognise and achieve their full potential

### **Our Values**

Excellence, Passion, Team Work, Integrity, Innovation,  
Sustainability, Valuing Others and Supportiveness

### **Sparsholt College Hampshire, incorporating Andover College**

The *Data Protection Policy* was approved by the Board of Governors  
in March 2018.

Next scheduled review: February 2021.

# DATA PROTECTION POLICY

*Integrity*

## **Contents**

1. Introduction
2. The Types of Information Covered by Data Protection Legislation
3. The College's Responsibilities
4. The Data Controller and the Designated Data Officers
5. The Rights of Individuals Whose Data is Processed by the College
6. Responsibilities of Staff
7. Responsibilities of Learners
8. Data Security
9. Loss or Theft of Personal Information
10. Subject Consent
11. Conclusion

## 1. Introduction

Sparsholt College Hampshire (“the College”) is registered as a Data Controller under the Data Protection Act 1998 and, from 25 May 2018, under the General Data Protection Regulation (GDPR). 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](http://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 1998 and, from 25 May 2018, the General Data Protection Regulation (hereafter referred to as the GDPR).

## 2. The Types of Information Covered by Data Protection Legislation

### Personal Data

Data Protection legislation applies to personal information 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.

### 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 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
- 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 information, and must make this clear in the privacy notice.

### **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 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 Human Resources Manager is the Data Officer for all data issues relating to staff.

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

### **5. The Rights of Individuals Whose Data is Processed by the College**

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

2. **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 exceptions being where the request is found to be unfounded, excessive or repetitive. See Section XX for details on how to access data.
3. **The right to rectification**  
Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
4. **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 information it holds.
5. **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
6. **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.
7. **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.
8. **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.

## 6. Responsibilities of Staff

- To ensure that any information that they provide to the College in connection with their employment is accurate and up to date.
- To inform 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 change 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).

## 7. 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 their Course Tutor.
- 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.

## 8. Data Security

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

- lock their IT device using -L or **[Ctrl]-[Alt]-[Delete]**, then **[Enter]** when leaving their PC/Surface/Laptop 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

- contact the Director of Information and Funding if in doubt about any data security matter
- 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).

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

## **9. Loss or Theft of Personal Information**

All incidences of loss or theft of personal information 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 information 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 information 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 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 will retain 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 information 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.

## **10. 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.

## **11. Conclusion**

Compliance with the 1998 Data Protection Act, and from 25<sup>th</sup> May 2018 the GDPR, 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 1998, the superseding General Data Protection Regulation, or how any aspect of either is implemented at Sparsholt College, please make contact with:

Data Protection Officer  
Sparsholt College  
Winchester  
SO21 2NF  
Tel: 01962 673288  
Email: [foi@sparsholt.ac.uk](mailto:foi@sparsholt.ac.uk)

**Related Policy:** SCH Freedom of Information 2000 Publication Scheme

**Useful Links:**

Information Commissioner: [www.ico.gov.uk](http://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>