

# IT 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 *IT Policy* was approved by the Board of Governors in April 2025 and supersedes previous versions of the IT Policy and IT Acceptable Use Policy

Originator:	Head of IT Services
Located:	College Group intranet
Due for review:	April 2028

# SPARSHOLT COLLEGE GROUP IT POLICY

## Contents

1. Introduction
2. Key Principles
3. IT Environment
4. IT Security
5. IT Equipment & Software
6. File Storage
7. Data Security
8. Account Authentication & Security
9. Loss or Theft of Confidential Information
10. Email Use
11. Internet Use
12. Campus Network
13. Remote Access
14. Personal IT Equipment
15. Monitoring & Logging
16. IT Acceptable Use
17. Use of Artificial Intelligence (AI) Applications

# SPARSHOLT COLLEGE GROUP IT POLICY

## 1. Introduction

This policy ensures the security and appropriate use of Sparsholt College Group's (the College's) IT systems. It applies to all students, staff, visitors, contractors, partners, and affiliates.

## 2. Key Principles

- 2.1 IT systems are protected against unauthorised access.
- 2.2 Users must comply with relevant data protection laws and associated college policies.
- 2.3 IT Services is responsible for system integrity and confidentiality.
- 2.4 Security breaches must be reported to IT Services immediately.
- 2.5 College-owned intellectual property must not be transferred without Strategic Leadership Team (SLT) approval.

## 3. IT Environment

- 3.1 IT Services manages all IT infrastructure.
- 3.2 All connections to the College network must comply with this policy.
- 3.3 Non-College-owned IT devices may connect if they comply with College guidelines as detailed in this document.

## 4. IT Security

- 4.1 Physical access to college data centres is restricted to IT Services, Premises and College Senior Leadership Team.
- 4.2 Mobile Device Management is utilised to track and secure mobile devices.
- 4.3 Log-on passwords are required for all College IT devices.
- 4.4 Users are responsible for securing equipment allocated to them by IT Services.
- 4.5 Unauthorised removable media storage is prohibited unless authorised by the College Leadership Team or Head of IT Services.
- 4.6 Cyber Essentials accreditation is required to be held and maintained by the College at all times.
- 4.7 IT Services and IT users are responsible for providing the security of the IT Infrastructure.
- 4.8 Users must log out or lock their computer when away from their desk.

- 4.9 Where practical, lock doors of offices containing IT equipment when left unattended and outside of general office hours and physically secure any unattended portable IT equipment.
- 4.10 When transporting College IT equipment, hide it from view and remove it when the vehicle is unoccupied.

## **5. IT Equipment & Software**

- 5.1 IT equipment is issued based on the purpose of its use and approved by the Head of IT services.
- 5.2 Software must be requested via IT Services.
- 5.3 Equipment must not be moved without IT Services approval.
- 5.4 All issued IT assets must be returned upon employment termination.
- 5.5 IT Services will maintain an asset register of all equipment.

## **6. File Storage**

- 6.1 The college provides both departmental and cloud storage for the storage of digital information. Files should not be stored in any other location.

## **7. Data Security**

- 7.1 Compliance with the Data Protection Act 2018 and GDPR is mandatory. The College will provide annual Data Protection and GDPR refreshers.
- 7.2 Records and information are sometimes required by law by external agencies and authorities. The Data Controller will comply with such requests on behalf of the College when formally submitted
- 7.3 Encryption, password policies, and secure disposal of IT assets are required.
- 7.4 Staff must not store College data on personal devices.
- 7.5 The Principal, Chief Operating Officer, and the Head of IT Services at the request of a Senior Post Holder may review the content of any logged College data on behalf of the organisation.
- 7.6 Data sharing is permitted for staff sharing with other members of staff using Teams, Email or Sharepoint. External data sharing is only permitted using email or Sharepoint (via IT Services). Consent to share data through any other method must be sought from the Head of IT Services.
- 7.7 Users are required to immediately notify IT Services if they believe that their IT account or device has been compromised.
- 7.8 IT Services are required to respond immediately to any notification of compromised hardware or software.

7.9 Staff and students should not attach College-owned devices to unsecured public WiFi networks unless they have no viable alternative.

## **8. Account Authentication & Security**

8.1 Username and password credentials must be kept secure and never shared.

8.2 Staff and student passwords must meet the detailed complexity requirements as set by IT.

8.3 Staff IT accounts will be created and suspended on the dates published in the starters and leavers list as provided by HR.

8.4 Student accounts are disabled within 24 hours of the student being withdrawn from all courses on ProSolution, or on the 90<sup>th</sup> day after their course completion date. 30 days after student accounts are disabled, the related OneDrive and email accounts are deleted in order to free up licences.

8.5 You are prohibited to use the IT account of another member of College staff or another student.

8.6 The College reserves the right to access, suspend or cease College accounts with permission from a Senior Post Holder.

8.7 Staff accounts are created with sufficient electronic privileges to enable users to carry out the work associated with their job roles. Any requests for enhanced privileges must be approved by Chief Operating Officer or Principal.

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

9.1 Loss or theft must be reported to the Director of Information and Funding immediately.

9.2 All Incidents involving security breaches are investigated and documented immediately upon their report.

## **10. Email Use**

10.1 Email is monitored for security, compliance and propriety, using external software.

10.2 Users must not send inappropriate or unauthorised messages.

10.3 External emails should be handled with caution.

10.4 Staff must not use personal email accounts for College business.

10.5 To preserve confidentiality of recipients' personal data, staff sending emails to groups of external recipients, must consider whether the email addresses should be assigned in the BCC field. For the avoidance of doubt, unless the recipients are already known to each other and have agreed to be disclosed to each other, the BCC field should be used.

10.6 IT users are required to apply care in dealing with any email that originates from outside of the College's network to ensure that they are accessing or reviewing information from a trusted source.

## **11. Internet Use**

11.1 The College may block access to certain websites the College considers may be inappropriate or harmful in an education setting.

11.2 Accessing illegal or inappropriate content is prohibited.

11.3 Web publishing of IT security details is prohibited.

## **12. Campus Network**

12.1 Personal devices must be approved before being allowed to connect to the network to ensure that the device has up to date security measures enabled and enacted.

12.2 Network traffic is logged and monitored for security.

12.3 Unauthorised network configurations will be prohibited by IT Services.

## **13. Remote Access**

13.1 VPN connections are restricted to College owned devices.

13.2 Remote access of the College IT system is logged and monitored for security purposes.

## **14. Personal IT Equipment**

14.1 Personally owned devices cannot connect to the College VPN.

14.2 Devices must have up-to-date antivirus protection to be allowed to access the College IT system.

14.3 IT Services will disconnect infected devices.

## **15. Monitoring & Logging**

15.1 All IT system usage is logged and monitored for security.

15.2 For the avoidance of doubt, online activities are monitored and enable the College to meet its Safeguarding and Prevent duty obligations.

## **16. IT Acceptable Use**

16.1 IT systems must not be used for illegal, offensive, or unauthorised activities.

- 16.2 Users must not attempt to gain unauthorised access or modify system data.
- 16.3 Personal use of IT systems is allowed but within reasonable limits which do not interfere with the users contractual requirements.
- 16.4 IT users must not transfer information from their personal email account to their College email account.
- 16.5 IT Users must not copy any data belonging to other users without their express and specific permission.
- 16.6 IT users must not use our computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for academic purposes which would require the fullest disclosure and special authorisations.)
- 16.7 IT users must not use College computing services to conduct any form of personal commercial activity without express permission.
- 16.8 IT users must not use, or attempt to use, the IT account of another member of college staff or another student.
- 16.9 IT users must not execute files, scripts or code known to be malicious.
- 16.10 IT users must not access the Dark Web, Tor Networks or Peer to Peer software.
- 16.11 College staff must use College email accounts for all business communication.
- 16.12 College data must not be stored on personal devices.
- 16.13 College staff requests for data transfer upon employment termination requires Senior Post Holder approval.

## **17. Use of Artificial Intelligence (AI) Applications**

- 17.1 AI tools must be used responsibly and in accordance with the College AI and Malpractice and Plagiarism policies.

This policy ensures a secure, efficient, and legally compliant IT environment at Sparsholt College Group.