SPARSHOLT COLLEGE GROUP

SPARSHOLT COLLEGE HAMPSHIRE

UNIVERSITY CENTRE SPARSHOLT

ANDOVER COLLEGE

IT Policy

Integrity • Sustainability

Our Mission

Raising Aspirations, Unlocking Potential, Advancing Futures

Our Values

Excellence, Passion, Team Work, Integrity, Innovation,

Sustainability, Valuing Others and Supportiveness

Sparsholt College Hampshire, incorporating Andover College

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 on 8 July 2021. It supercedes all previous versions and is effective immediately.

Originator:	IT Manager
Located:	College websites
	College Group intranet
Due for review:	March 2023

IT Policy

Integrity, Sustainability

Table of Contents

IT Policy

1 Introduction

This policy defines a framework which protects the College Group's computer systems, assets, infrastructure and computing environment from threats, whether internal, external, deliberate or accidental.

For the purposes of this document the following terms apply:

- IT – Information Technology, including physical hardware, software and provided services
- ITS – the IT Services Department
- Intranet – Internal Web based information supplied via browser
- SLT – the Strategic Leadership Team
- College – all parts of the College Group

Ignorance of this policy and the responsibilities placed on you is not an excuse in any situation where it is assessed that you have breached the terms set. Breach of this policy may be dealt with under our Disciplinary Procedures and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

The IT Policy is covered in student induction.

Staff are advised of this document during their induction and of the College's requirement for them to adhere to the conditions therein. Staff are expected to refresh their knowledge of the policy periodically to keep abreast of changes. An up-to-date version can be found on the Policies page of the Intranet (Sharepoint).

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

All users have a responsibility to report promptly to ITS, any incidents which may have an IT security implication for the College.

This policy applies to:

- Students
- Staff
- Visitors
- Guests
- Contractors
- Partners and Affiliates of the College

Staff are responsible for ensuring anyone within their area of responsibility is complying with this policy.

2 Key Principles

All IT systems and information contained within them will be protected against unauthorised access.

All users of our IT facilities are required to comply with this policy.

When using our IT services you must at all times comply with the law of the land.

Information kept within College systems will be managed securely, to comply with relevant data protection laws and to satisfy our expectations that such assets will be managed in a professional, safe and dependable manner.

All employees and students of the College are required to familiarise themselves with this policy and comply with its requirements.

Managers and staff with a supervisory responsibility have a responsibility for ensuring adherence to and compliance with this policy throughout their areas of responsibility.

The integrity of all IT systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of ITS.

All regulatory and legislative requirements regarding computer security and IT based information, confidentiality and integrity will be addressed by ITS.

All breaches of security will be reported to and initially investigated by ITS.

The College owns all intellectual property / capital / connect in perpetuity that is produced and stored on College computing services assets. As such, at the end of employment contracts, members of staff are not permitted to transfer any data from College servers, systems or databases without express agreement from a member of the College Strategic Leadership Team.

3 The IT Environment

ITS manages, maintains and operates a range of IT equipment including, Servers, Switches, Routers, Firewalls, Backup Systems and the overall Network Infrastructure interconnecting these systems.

The IT environment is defined as all IT resources, Software, Data, Physical and Network Infrastructure managed and overseen by ITS and all devices that can physically connect to it, and that have been authorised to connect to it. This policy covers the entire IT environment.

All connections to the College infrastructure, be they temporary or permanent, via our physical network, wireless network, or remote working connections, are subject to the conditions of this policy.

IT resources not owned by the College, may be connected to our network. However, all such resources must comply with our guidance governing the use of IT resources.

IT will log, collect and analyse the content of all transmissions on the College networks for performance, fault diagnostic and compliance purposes.

4 Physical Safety

All IT is supplied in a working state. Visual inspections of all IT equipment should be carried out before use; any equipment found not to be working, or suspected of being faulty or damaged, should be reported immediately to the ITS Service Desk.

Open drinks containers, cups, beakers, etc. should not be within 1 metre of any IT equipment.

5 IT Security

To secure the IT estate, IT Services will:

- restrict and monitor physical access to data centres
- run a Mobile Device Management Suite to track and trace the location of the majority of mobile devices or wipe devices should they become compromised.
- use devices or mechanisms for securing and protecting IT equipment main components and contents from theft
- enforce use of a log-on or power-on password on portable IT equipment wherever possible

Members of staff are responsible for the security of the equipment allocated to or used by them, and they must not allow it to be used by anyone other than in accordance with this policy. They should use passwords on all IT equipment, particularly items that they take out of the office. They should keep their passwords confidential and change them regularly.

In order to ensure the security of the College IT estate, staff are expected to:

- log on to the College's systems using their own username and password. Staff must not use another person's username and password or allow anyone else to log on using their username and password
- log out or lock their computer when away from their desk. Staff must log out and shut down their computer at the end of each working day
- where practical, lock doors of offices containing IT equipment when left unattended and outside of general office hours
- physically secure any unattended portable IT equipment - for example locked in an office or a desk drawer
- hide any portable equipment from view when being transported in a vehicle, and remove it when the vehicle is unoccupied e.g. overnight

Removable media, USB memory sticks, etc, must not be used to store any personal information. Staff should contact IT Services for advice if they feel they have a requirement to do so.

Staff must not store College-owned personal information on personally owned portable equipment. Please contact the IT Manager or the Director of Information & Funding for advice if required.

The College is working towards Cyber Essentials (CE) accreditation, and additional protective measures will be put in place during the lifetime of this policy as a result of the requirements of the CE framework.

6 Provision of IT Equipment and Software

IT equipment is supplied on receipt of requests from Assistant Principals or Cost Centre Managers with approval from their appropriate SLT member.

Academic staff

- Up to .6 fte – Issued with appropriate portable device
- Less than .6 fte and Sessional – To use portable device from departmental pool

A set of IT applications available to all staff can be found by accessing the Software Centre of your device via the Windows menu. Any required application neither pre-installed on your device nor available in the Software Centre should be requested from the IT Service Desk.

Where IT equipment is positioned and installed by IT Services it is not to be moved without IT Services assistance and approval.

Damage to any IT equipment must be reported to the IT Service Desk at the earliest opportunity.

IT Services will maintain a register of portable equipment that is issued to staff, and staff will sign for all such equipment.

At the end of your employment all College assets, including any peripherals, must be returned in good working order, and signed back in to IT Services.

7 File Storage

You have access to a centrally managed file storage facility via personal and shared drives.

Personal Home drive storage, sometimes referred to as the 'Z Drive', is limited to 3GB for staff users and nominally 250MB for Students. OneDrive for Business storage for all users is set to 1TB.

Personal/home drive storage should only be used for your personal data and data that no-one else has a requirement to access.

Shared/departmental storage should be used for all other storage.

Access rights to all data is maintained by ITS to guidance from the data owners or SLT.

Use of any cloud-based file storage other than OneDrive for Business, as provided by us, is strictly forbidden. Any use of such breaches our policy on safeguarding information.

The use of removable media in the form of memory sticks as the sole location for storing data is strongly discouraged. Data loss through physical loss or corruption of data is commonplace on such items. Personal/sensitive data must not be stored on such media.

8 Data Security

All use and processing of personal information and data is governed by the auspices of the Data Protection Act 2018 and the General Data Protection Regulation 2016 (GDPR). Staff are reminded of their responsibilities under the Act and the future GDPR in maintaining the security and preventing the unauthorised disclosure of any personal data held.

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

- 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 expected to:

- lock their IT device using **Windows-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).

Individuals should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

Individuals must not download or install software from external sources without authorisation from ITS. Downloading unauthorised software may interfere with the College's systems and may introduce viruses or other malware.

Staff must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the IT department.

Private and personal non-work-related media, data, documents and records should not be saved to any College servers, systems or databases.

Staff and students must not view, access or transmit confidential information about the organisation including any of our staff or students (except as authorised in the proper performance of your duties).

Staff and students must not attached College-owned devices to unsecured public WiFi networks.

9 Account Authentication

Access to the secure areas of the network is controlled by Username and password; these are issued at either contract start or course start. Accounts will be disabled within a reasonable time of contract end or course completion. Account security is paramount to system security - **never give your password to anyone**.

Staff usernames are composed of the first initial and surname (e.g. Joe Bloggs: jbloggs)

Student usernames are the student ID numbers only (e.g. ABC12345678: 12345678)

Staff Passwords must:

- Be a minimum of 8 characters long.
- Contain at least 3 character sets (uppercase, lowercase, numeric, special).
- Not contain the Username.
- Not be the same as the last 8 passwords.
- Be changed every 90 days.

Student passwords must:

- Be a minimum of 6 characters long.
- Contain at least 3 character sets (Uppercase, Lowercase, Numeric, Special).
- Not contain the Username.
- Not be the same as the last 8 passwords.
- Be changed once a year.

College systems Administrator accounts will be set up for Multi Factor Authentication (MFA).

10 Account Security

Access to our IT systems is via a Username and secure password. It is your responsibility to keep your password secure. ITS cannot see your password but can, on request, reset it for you either by request in person to the service desk with your college ID, or by having your manager (in the case of staff members) or lecturer/tutor (in the case of students) send a request via email.

Passwords must be

- Minimum 8 characters long.
- Contain at least 3 character sets (uppercase letters, lowercase letters, numbers, special characters).
- Not contain your username.
- Changed every 90 days for staff.
- Not be the same as your last 8 passwords.

You are probibited to use the IT account of another member of college staff or another student.

- A member of SLT, must provide written confirmation to ITS to allow us to grant access to a staff account in the event of leave or sickness and where required for the operation of the college.
- The College reserves the right to access, suspend or cease College accounts with permission from a Senior Post Holder.

Staff IT accounts will be created and suspended on the dates published in the starters and leavers list as provided by HR, unless specifically requested by the appropriate Cost Cente Manager to the IT Manager. However, as part of the College's safeguarding process no IT account for staff/agency staff/self-employed/contractors will be set up unless permission is given by the HR department.

Student IT accounts are created automatically after the student is enrolled on ProSolution. Student accounts are disabled within 24 hours of the student being withdrawn from all courses on ProSolution, or on the 90th 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.

11 Loss or Theft of Confidential Information

All incidences of loss or theft of confidential 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 confidential 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.
- The availability of the system or information being put at risk.
- Adverse impact, e.g. Negative impact on the reputation of the College.
- Threat to personal safety or privacy.
- Legal obligation or penalty.
- Financial loss or disruption of activities.

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 serious 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 or other third parties, e.g. insurers. The Data Controller will retain a central register of all such incidents occurring within the College.

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 breach of security:

- Loss of computer equipment due to crime or carelessness.
- Loss of portable media devices (memory sticks etc.) containing personal data.
- Accessing any part of a database using someone else's password.

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.

12 Email

Email is provided for all staff and students. The College's email system, including records of Instant Messenger (IM) conversations, is a searchable data system, and as such is subject to disclosure of content about identifiable individual people.

Email is not a completely secure medium. You should be conscious of this and consider how emails might be used by others. Remember that emails can easily be taken out of context, that once an email is sent you cannot control what the recipients might do with it, and that it is very easy to forward large amounts of information.

You should not necessarily trust what you receive in an email - in particular, you must never respond to an email request to give a username or password. Any such emails should be referred to ITS.

Take extra care in dealing with any email that originates from outside of the College's network (a red banner at the top of the email will announce its external nature).

Protect the College's cyber security by taking care when clicking on URL links in emails or opening attachment files.

Inform IT Services of any suspicious emails received, so that the originator can be blocked if necessary.

You need to be aware that any messages deemed to bring the College's name into disrepute will be treated and investigated as a disciplinary matter.

Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. Employees should also include the College's standard e-mail signature and disclaimer.

Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

Individuals must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

Employees should not:

(a) send or forward private e-mails at work which they would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or

(d) send messages from another person's e-mail address (unless authorised) or under an assumed name.

Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account provided by the college for this purpose.

The College monitors all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it

You should inform the IT service desk immediately if you suspect that your computer has a virus.

With the consent of IT your college email can be retrieved on your own personal device but in doing so your device has to comply with this IT policy. Consent and Instructions can be obtained from the IT Service Desk.

13 The Internet

Consider the security implications of any information you put on our Website or Virtual Learning Environment.

You should not in any way use any areas of our Website for commercial purposes not related to the College's business.

You shall not in any way use web space to publish material which undermines IT security at the College. In particular this covers making information available about how IT security is implemented at a practical level, or any known weaknesses.

Individuals should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that the

College's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Any use of the internet must also comply with obligations detailed in the E-Safety and Online Communications policies for staff and learners.

We reserve the right, without warning, to block access to external web services, where we deem it appropriate to do so.

14 Campus Network

You must seek permission from ITS before physically connecting any form of IT device to the physical College network.

Any device connected to our IT network can be removed without warning for breaching the IT policy.

All network traffic may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised personnel, are kept for no longer than necessary and in line with current data protection guidance.

Such records and information are sometimes required - under law - by external agencies and authorities. The Data Controller will comply with such requests on behalf of the College when formally submitted.

For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

b) to find lost messages or to retrieve messages lost due to computer failure;

c) to assist in the investigation of alleged wrongdoing; or

d) to comply with any legal obligation.

The only protocol family supported by IT Services is TCP/IP. You must not run or allow to be run:

- DHCP servers
- DNS Servers
- Routing Protocols (such as OSPF, RIP etc)
- Network Discovery Protocols
- Internet Connection Sharing
- Port Scanners

Neither are you permitted to:

- Attempt DDNS dynamic Name Server Updates.
- Set up network file shares that are writable without a password.
- Re-distribute network access to others, nor any College resource made available to them.
- Configure any device attached to the Network with any IP address not specifically allocated to them.
- Connect any form of Wireless Access point to the Network, nor configure any computer with wireless capability such that the Network can be accessed wirelessly.
- Download or distribute copyright material in breach of any licence conditions.
- Run Peer to Peer applications that distribute copyright material.
- Use proxy services to circumvent network security.

15 Remote Access to Systems

Remote access is defined as accessing systems from a physically separate network. This may include:

- Direct connections across the Internet.
- VPN (Virtual Private Network) connection.

Any user with a valid College IT account may access systems as appropriate using a college owned device. Remote access is allowed via secure methods only.

Remote connections to any campus IT service is subject to the same rules and regulations, policies and practices just as if they were physically on the campus. IT Services provide the only VPN service that may be used.

All connections via these services will be logged. No other remote access service shall be installed or set up, including single modems connected to servers or workstations. Any active dial-in services found to be in existence will be removed from the network.

16 Personal IT Equipment

You are not permitted to access the College VPN via personally owned devices.

When connected to our IT network, you must ensure that you are running with adequate and up-to-date anti-virus software at all times. If the IT Services team detect a device behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

17 Anti-Virus Security

When connected to our IT network, you must ensure that you are running with adequate and up-to-date anti-virus software at all times. If you suspect viral or malware infection on your machine, a complete security scan should be performed. Should IT Services detect a device behaving abnormally due to a possible infection it will be

disconnected from the network until deemed safe. Reconnection will usually only be after direct liaison with IT Services.

18 Monitoring and Logging (Including Safeguarding and PREVENT Obligations)

All activities can and will be monitored and logged from time to time for security, diagnostic and account / audit reasons. Logs are only available to authorised individuals and retained for no longer than necessary.

Such records and information are sometimes required - under law - by external agencies and authorities. We will comply with such requests when formally submitted.
When using portable IT equipment we have the ability to monitor and record its, and therefore your, physical location.

The following activity is actively monitored and logged as part of the College's responsibility towards multiagency PREVENT obligations:

- Information which may lead to potential terrorism or extremist activity.
- Internet activity on sites classified under the following categories:
    - Intolerance
    - Personal weapons
    - Terrorism
    - Violence
    - Radicalisation

Logs and information relating to Safeguarding or Prevent will be monitored by the College's Safeguarding Team, and may be shared with other authorities for further investigation. Specific permission to access internet material relating to any of these categories for academic purposes should be sought from the College's Strategic Leadership Team where required.

19 Additonal Acceptable Use Requirements

When using our IT services you must NOT:

- Attempt to create, circumvent or elevate permissions of user accounts.
- Access any program or data which has not been specifically authorised for your use.
- Use or copy any data or program belonging to other users without their express and specific permission.
- Alter computer material belonging to another user without the user's permission.
- Use our computing services to harass, defame, libel, slander, intimidate,

impersonate or otherwise abuse another person.

- 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)
- Use our computing services to conduct any form of non college related commercial activity without express permission.
- Use our computing services to disseminate mass (unsolicited) mailings.
- Install, use or distribute software for which you do not have a licence.
- Execute files, scripts or code known to be malicious.
- Access the Dark Web, Tor Networks or Peer to Peer software (e.g. BitTorrent).
- Create, view, access, transmit or download material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities policies, Bullying and Harassment policies for staff and learners, or Sexual Misconduct Policy and which is likely to create any criminal or civil liability (for you or us).