SPARSHOLT COLLEGE GROUP

SPARSHOLT COLLEGE HAMPSHIRE

UNIVERSITY CENTRE SPARSHOLT

ANDOVER COLLEGE

IT Acceptable Use Policy

Excellence • Integrity • Supportiveness

Our Mission

Raising Aspirations, Unlocking Potential, Advancing Futures

Our Values

Excellence, Passion, Teamwork, 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 Acceptable Use Policy was approved by the Board of Governors in April 2023 and supersedes previous versions.

Originator:	IT Services Manager
Located:	College website College Group intranet
Due for review:	February (for April) 2025

IT ACCEPTABLE USE POLICY

Excellence, Integrity, Supportiveness

Contents

IT ACCEPTABLE USE POLICY

1. Introduction

This policy sets out what constitutes acceptable use of the College Group's (the College's) IT systems and should be used in conjunction with the College Group's IT Policy and Data Protection Policy. To use the College Group IT Resources, users must agree to the responsibilities and conditions outlined in this IT Acceptable Use Policy.

2. General

Access to the College Group IT Resources is available via a User Account associated with an individual user.

When using our IT services you must at all times comply with the law.
When using our IT services you must NOT:

- Use a computer that you have not been authorised to use.
- Interfere with any others' use of these facilities and services.
- 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 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.
- Use, or attempt to use, the IT account of another member of college staff or another student.
- Execute files, scripts or code known to be malicious.
- Access the Dark Web, Tor Networks or Peer to Peer software (e.g. BitTorrent).

Users should remember:

- The College owns all intellectual property / capital / connect in perpetuity that is produced and stored on College computing services assets.

- The College reserves the right to access your College account with permission from the HR Manager / Head of Department / Faculty and a member of the Strategic Leadership Team (SLT).
- In general, use of College computing services should be for your study, research, teaching or the administrative purposes of the College. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.
- Use of College computing services for your own commercial work may be governed by software licence constraints, and users should verify with IT Services staff that the intended use is permissible under the terms of those licences.
- You should take all appropriate precautions to prevent unauthorised access to your user account, ensuring you do not share, loan, publish or expose the access details.
- Users are responsible for any electronic activity that originates from sessions that were logged in using their account.
- If you think your account has been compromised, change the password and contact the IT Service Desk for advice.

3. 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) wherever possible.

4. Safe and Secure Usage

When accessing and using College IT systems, users should do so in a safe and secure manner. In particular, users should:

- Keep their passwords secret.
- Lock any device that they are logged into when leaving the device unattended.
- 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.
- Take care that personal or private information displayed on screens is not visible to others who are not entitled to view it.

5. Data Storage

Files can be saved to the provided drives; limited space is available so users should be aware of space constraints and save to shared areas where possible. Space is provided for each user on a Personal / Home / Z drive, and files that cannot be stored in shared areas can be stored in those areas.

- Students – 250Mb
- Staff – 3Gb

Students have a further 100Gb of storage available on OneDrive. Use of any cloud-based file storage other than OneDrive, as provided by us, is strictly forbidden. Any use of such, breaches our policy on safeguarding information. The use of USB memory sticks is strongly discouraged - they break and lose data very easily. The use of unencrypted USB memory sticks to store any personal data that is not your own is forbidden.

6. 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.
Access to the email account or personal drive of another user will only be granted with the express permission of a member of the SLT.

7. Personal IT equipment

7.1 Anti-Virus
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

7.2 Remote Connections
Any user with a valid College IT account may access systems as appropriate. Remote access is only allowed via the secure methods we supply. Remote connections to any campus IT services are subject to the same rules and regulations, policies and practices as if they were physically on the campus. All remote connection attempts will be logged.

7.3 Firewalls on Personal Devices
When using a personal device to access organisational resources you must ensure that you have a valid firewall enabled.

8. Monitoring and Logging

A condition of your logging into the College's IT systems is that you agree that data identifying you as an individual and detailing your activity can be securely stored by the College, and, if necessary, used to investigate breaches of this policy.
All activities can and will be monitored and logged for security, diagnostic and account / audit reasons, and for specific purposes such as safeguarding and PREVENT. 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 College monitors internet use electronically, via computer programs that watch for suspicious key words. Users should take care not to access inappropriate material online, but if such material is accessed inadvertently then the IT Services team should be informed so as to account for the activity.

9. Safeguarding and PREVENT

The following activity is actively monitored and logged as part of the Colleges responsibility towards multiagency safeguarding and PREVENT agendas:

- 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
- Information which may lead to a potential risk to young people or vulnerable adults.
- Internet activity on sites classified under the following categories:
    - Adult entertainment
    - Adult sites
    - Child abuse
    - Pornography

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 Senior Leadership Team where required.

10. Staff Usage

College Information Systems are for use on College business only. Staff must not use College Information Systems to access information for private or non-College-related use or activity.

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.

When accessing College Information Systems via personal devices, College data should not be downloaded to the personal device.

College-owned devices should not be attached to unsecured public WiFi networks.
Remote access to the College Domain is only available via equipment owned by the College. VPN access should not be attempted via personally owned devices.

When members of staff send emails to groups of external recipients, consideration should be given to whether or not the email addresses should be assigned in the BCC field, in order to preserve confidentiality of recipients' personal data.

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

At the end of employment contracts, members of staff are not permitted to transfer any data from College servers, systems or databases without agreement from the HR department.

Related College Group Policies:

- IT Policy
- Data Protection Policy