SPARSHOLT COLLEGE HAMPSHIRE

ANDOVER COLLEGE prepared for life

E-Safety and Online Communications Policy (Learner Version)

Excellence, Integrity, Supportiveness

Principal: Tim Jackson BTech (Hons), PGCE

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 *E-Safety and Online Communications Policy* was approved by the Board of Governors in April 2020. This supersedes any previous publication and is effective from April 2020.

Equality Impact Assessment	Conducted:
Originator: Deputy Principal Curriculum	Located: College Document Library
	College Intranet
	College Website
Date of next scheduled review: *March 2022*	

E-Safety and Online Communications Policy

Excellence, Integrity, Supportiveness

Contents **Page**

1. Policy Statement

Sparsholt College Group recognises the benefits and opportunities that new technologies offer to teaching and learning. Our College encourages the use of technology to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that learners (and our staff, through their version of this policy) are also aware of potential risks and challenges associated with such use.

The College is committed to enabling appropriate access to and responsible use of social media within the realms of our Safeguarding Learners Policies and Procedures. With the now widespread use of online communication (incorporating all social media) such as Facebook, Instagram, Snap Chat, You Tube, Twitter and Tik tok, amongst many others, this raises a potential area of concern for the College.

Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently. The College believes this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In furtherance of our duty to safeguard learners and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care.

This E-Safety and Online Communications Policy should be read in conjunction with other relevant College policies including the Student Code of Conduct, IT Policy (incorporating Acceptable Use), Safeguarding Learners, Managing Learner/Student Conduct, and Bullying and Harassment Policy.

2. Policy Scope

This policy covers:

- All learners logging into any network, service, website or portal associated with Sparsholt College group.
- Connecting a device via the Sparsholt College Group network.
- Any electronic communication with a Sparsholt College Group Learner or member of Staff.
- From any geographic location both on Campus and off Campus.
- The use of social media in all contexts and forms at Sparsholt College and Andover College (“the College”).

3. Roles and Responsibilities

All learners:

- MUST keep to the terms and conditions of the IT Acceptable Use Policy at all times.
- Must receive appropriate e-safety guidance as part of their programme of study.
- Inform a member of staff where they are worried or concerned an e-safety incident has taken place involving them or another member of the college community.

- Must act safely and responsibly at all times when using the internet and/or mobile technologies

4. Behaviour

Use of any Sparsholt College Group IT equipment and systems is conditional to the College Policies including the IT Policy and Bullying & Harassment Policy and Procedures.

Communications between learners or with staff should be courteous and respectful at all times whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Bullying and Harassment Policy and the Student Code of Conduct.

Cyber Bullying

Cyber bullying is a form of bullying. As it takes place online, it is not confined to College buildings or College hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

Cyber bullying includes bullying via:

- **Text message and messaging apps** e.g. sending unwelcome texts or messages that are threatening or cause discomfort.
- **Picture/video-clips** e.g. using mobile device cameras to bully someone, with images usually sent to other people or websites.
- **Phone call** e.g. silent calls or abusive messages. The bully often disguises their number.
- **Email** e.g. emailing upsetting messages, often using a different name for anonymity or using someone else's name to pin the blame on them.
- **Chat room** e.g. sending upsetting responses to people when they are in a web-based chat room.
- **Instant Messaging** (IM) e.g. sending unpleasant messages in real-time conversations on the internet.
- **Websites** e.g. insulting blogs, personal websites, social networking sites and online personal polling sites.

Where conduct is found to be unacceptable, the College will deal with the matter internally and refer to relevant policies, for example, the Managing Learner/Student Conduct. Where conduct is considered illegal, the College will report the matter to the police.

5. Monitoring

The College has the right to monitor, log and report on learners and staff use of its computer and communication systems that are made available to staff and learners as part of the College's responsibility towards the 'Safeguarding of young people and vulnerable adults' and Prevent Duty.

An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the College's policy on Managing Learner/Student Conduct.

Where requested this information will be securely shared with appropriate local authorities and external support agencies.

6. Cyber Security

In line with the ESFA condition of funding for 2020-21, Sparsholt College Group is documenting compliance with the tenets of the Cyber Essentials scheme, with a deadline of achieving certification before August 2020. The IT Services department are confident that the College already works to and beyond the 5 standards set by the Cyber Essentials scheme:

- **Secure your Internet connection.** We have our internet connection secured via a Firewall at each campus, and by using software for monitoring electronic traffic and preventing access to inappropriate websites or material. An external company is engaged to undertake penetration testing of the College's IT systems.

- **Secure your devices and software.** Mobile devices have 2-stage protection to prevent unauthorised access. Various group policies are applied to all devices to restrict what users can do, and password policies are in place with expiration times and minimum levels of complexity.

- **Control access to your data and services.** All user accounts are managed within Group Policy security groups, only allowing access to locations and data they need to access. Software is only installed on devices where it is required, on a centrally controlled basis.

- **Protect from viruses and other malware.** The College uses security software, updated daily, to protect desktop computers, mobile devices and servers. We have implemented controls to prevent file types with defined extensions from being accessed or run, as well as specific programs/apps. An electronic ban has been implemented on the running of executable software from all removable media (including USB), to protect the IT Systems from the introduction of malware.

- **Keep your devices and software up to date.** The College's IT estate's currency is maintained via the implementation of security patches and software/hardware updates by the IT Services team.

The electronic security standard for meeting the ESFA's condition of funding will move to Cyber Essentials Plus for the 2021-22 academic year, with full certification against ISO 27001 (Information Security) planned to become the required standard for a later year to be determined. The College is developing plans to develop its cyber security in line with the ESFA timeline.

The College will do all that it can to make sure the College systems are safe and secure. Every effort will be made to keep security systems effective and up to date. All digital transactions on the College network, including email and internal postings, will be recorded by the IT Services team.

Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring / accessing someone else's digital identity is a criminal offence and will be referred to the College's policy on Managing Learner/Student Conduct and sent to the police for investigation.

7. Safeguarding and Prevent

All learners will be taught how to stay safe online and encouraged to take responsibility for their own and others' safety. The College aims to empower learners to become safe, responsible digital citizens with the ability to assess risk for themselves, wherever and whenever they are using ICT. All learners will be taught how to recognize when they are at risk and know where to go for help when they need it.

8. Remote teaching and learning

The college will, on occasions, use a blended learning approach involving delivery of learning via an online platform. Where live classes take place (i.e. via Big Blue Button or Teams) these lessons will be recorded and backed up on the College servers.

Learners are reminded that this is a professional environment and therefore must behave in line with the student Code of Conduct. Students must wear suitable clothing, and use appropriate language at all times during these lessons

9. Training

Learners will be provided with e-safety guidance by personal tutors and have access to e-safety information on the Student intranet (Moodle Badge). Tutorial planning will include appropriate and relevant e- safety guidance for learners and will also ensure learners consider their digital footprint in both a personal and professional context.

Issues associated with e-safety apply across the curriculum and learners will receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the college e-safety expectations will appear when users log on to the college network as well as highlighting e-safety themes within tutorial and awareness campaigns throughout the academic year.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

10. Online Communication

The appropriate use of communication applies to all devices and services, which might include:

- Computers, Laptops & Mobile devices (including phones and tablets)
- Game Consoles
- Email, Instant / Direct Messages & Chat rooms
- Social Media

The points below offer guidance on appropriate use of online communication and any breach of this guidance will be referred to the College's policy on Managing Learner/Student Conduct. Any breach considered to be a criminal offence will be referred to the police for investigation.

- You must not create, store, exchange, display, print or circulate any message or media which may cause offence to others.
- You must not send messages at random or excessively, also referred to as "spamming".
- You should not open files or emails from people you do not know. They may contain viruses or offensive material.
- You should not save your log-on details on shared computers as some people may use your screen name to defraud or scam people in your contact lists.
- There may be legal implications if the Internet is used for criminal intentions for example to intimidate or to extract financial information for personal gain. All conversations using college IT

systems are captured and recorded on the college's servers.

- You must own the copyright of any material you post.

11. Social Media

Creating new social media accounts

New social media accounts that use an official logo or reference any part of the Sparsholt College Group must not be created unless approved through the College's social media approval process.

The Marketing team must be given administrator access to social media accounts which appear to represent the College Group or an aspect of its provision.

The College will close down any "unofficial" social media sites using the College's logo, name or copyrighted materials, even if created by staff or learners.

Guidelines for Responsible Use of Social Media

Sparsholt College learners must be aware of their social media presence, particularly when the social media account openly states that they study within the Sparsholt College Group. If a student discloses their affiliation with the College on their profile or in any social media postings, they must ensure that any content they post is appropriate and in line with the College's values.

Your social media presence on sites such as Facebook can contain a lot of personal information that you might not wish to share with all of your peers or the general public. Unless your privacy settings are restricted, your peers may be able to access your personal information. Therefore, it is important to ensure that your privacy settings reflect the amount of information you want people to find out about you.

It is recommended that other online personal profiles are set to the maximum possible security settings. This means that only you and people in your friends and/or followers list will be able to see the updates you post.

Be respectful to others when making any statement on social media and be aware that everyone individually is personally responsible for all communications which will be published on the internet for anyone to see.

If you see social media content that disparages or reflects poorly on the College, you should contact your tutor.

College Reputation

Sparsholt College Group learners are expected to respect the College's reputation when posting online. It would be inappropriate to:

- Post any material critical of the College, learners or staff on any social media site.
- Post comments that run counter to the Colleges Values and/ or its Equality and Diversity policies.
- Post comments that condone, or appear to recommend, law-breaking of any kind.
- Harass, bully or unlawfully discriminate against fellow learners, staff or third parties.

Any information which may be consider damaging to the College's reputation may result in disciplinary

and/or legal action.

Accepting friends/followers

Staff of Sparsholt College Group must maintain professional boundaries at all times, and are therefore not able to accept 'friend' connections from their learners on personal social media accounts.

Exceptions to this rule can be made when the primary connection between a member of staff and a restricted person does not stem from them being a learner of, or from interactions within, the College Group, and this has been declared as an expression of interest to the DSL.

Social Media in Teaching and Learning

Social media may be used to reach learners to inform them of course related activities, events and news. Social media can be used to enhance a learner's experience through carefully planned use in teaching and learning, however will not be the primary learning environment for learners.

Course content, collaborative working, group discussion and class level communication will be based within the agreed College learning and working environments. For teaching and learning, Moodle, Ledge, Mahara, eStream, Wam (including Linked Ledge), Microsoft packages including MS Teams, One Drive, Stream and Class notebook are the College's chosen digital learning and working environments.

All learners will have a Sparsholt College IT account, providing access to these digital learning and working environments. Internal technical support, guidance and training are also available to users of these platforms through IT helpdesk, the Create Hub, the Library team and Learning Technologists.

Learners are not obliged to create social media accounts in order to access course materials and learners should not be disadvantaged by choosing not to participate within a social media platform.

Approved Social Media Channels

The following social media channels are maintained by the College's Marketing department:

- Facebook:

  https://www.facebook.com/SparsholtCollege
  https://www.facebook.com/AndoverCollege
  https://www.facebook.com/UniCentreSparsholt

  Other Facebook pages may represent the commercial activity of the College.

- Twitter:

  @AndoverCollege
  @Sparsholt_Coll
  @UC_Sparsholt

- Instagram

  Sparsholt_Coll
  Andover_college
  uc_sparsholt

- Wambiz: Sparsholt.wameducation.com

12. Copyright

- Students are responsible for ensuring they have the appropriate copyright licence for the use of any content or media being used.
- All copyrighted material must be obtained from a legitimate licensed source.
- The distribution of material which infringes copyright is a criminal offence and will be referred to the College's disciplinary Managing Learner/Student Conduct and/or the police for investigation.
- The use of file sharing software including but not limited to Bit torrent is forbidden over the College network.
- The use of any website must be used within accordance of the website terms and conditions.
- The downloading of YouTube videos for offline use is not permitted by the terms and conditions of the website.

13. Use of Images and video

There are particular risks where personal images are posted onto online communications. The College's aim is to reinforce good practice as well as to offer further information for all users on how to keep their personal information safe.

No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner of that image. Photographs of activities on the College premises should be considered carefully before being published. Approved photographs and imagery should not include names of individuals.

14. Personal Information

Personal information will be held and processed in accordance with the General Data Protection Regulation (GDPR) 2018.

For more information please refer to the Sparsholt College Data Privacy Notices available on the website www.sparsholt.ac.uk

15. Breach of this Policy

Breach of this Policy may result in disciplinary action up to and including exclusion.