E-Safety and ICT Acceptable Usage Guidance

For clarity, this guidance uses the following terms unless otherwise stated:

Users - refers to staff, Academy Governance Committee (AGC), college volunteers, students and any other person working in or on behalf of the college, including contractors.

Parents – any adult with a legal responsibility for the student/young person outside the college e.g. parent, guardian, carer.

College – any college business or activity conducted on or off the college site, e.g. visits, conferences, college trips etc.

Wider college community – students, all staff, Academy Governance Committee, parents.

Safeguarding is a serious matter at S6C (Salisbury 6th Form College). We use technology extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such, this guidance is reviewed on a regular basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this guidance is twofold:

- To ensure S6C meets the requirement to empower the whole college community with the knowledge to stay safe and risk free.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the college.

This guidance is available for anybody to read on the S6C website

Introduction

The online world is second nature to many of our students and we respect their knowledge. That said, however familiar and comfortable we are online, safety is exceptionally important.

Staff and students should be aware that, although a wonderful resource, online activity, (including but not limited to social media) needs to be managed very deliberately in order to avoid potential harm.

This harm could include unexpected friendship issues, bullying, blackmail, prejudice and abuse, sexual or financial exploitation, sexual abuse, criminal recruitment, catfishing, scams and fraud, misinformation and fake news, the impact of your digital footprint on future plans, trolling, exposure to damaging and unhelpful content, and even criminal conviction if students do not know the current laws around issues such as consensual and non consensual sharing of nude and semi nude images.

We encourage students to think very carefully about these issues - to read and think about the information we share, even if they feel they know how to keep themselves safe.

Keeping Children Safe in Education 2023 identifies:

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism (Prevent Duty).
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group **apwg.org**

Online Safety within the Life Skills Programme

Online safety is taught in Life Skills in the first half term of each academic year with a foundation in Year 12 and a recap and extension session in Year 13.

Online safety is also signposted before college holidays and when entering a period of extended online learning.

The presentation and resources for students can be accessed any time in the Google Information Classroom. Information is also shared with parents/carers via our Weekly Update.

Roles & Responsibilities

Academy Governance Committee (AGC)

The AGC is accountable for ensuring that our college has effective policies and procedures in place; as such, they will:

- Review this guidance periodically and in response to any e-safety incident to ensure that the guidance is up to date, covers all aspects of technology use within the college, to ensure e-safety incidents were appropriately dealt with and ensure the guidance was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-safety at the college who will:
  o Keep up to date with emerging risks and threats through technology use.
  o Receive regular updates from the Head of College in regards to training, identified risks and any incidents.
  o Report to Governors at the AGC Meetings

Head of College

Reporting to the MLP CEO, the Head of College has overall responsibility for e-safety within our college. The day-to-day management is delegated to an outside Agency (Oakford - IT Supplier for MLP).

The Head of College will ensure that:

- Appropriate ICT training throughout the college is planned, up to date, and appropriate to the recipient, i.e. students, all staff, senior leadership team and AGC, parents.
- The designated IT Support Agency has had appropriate CPD in order to undertake the day-to-day duties.
- All e-safety incidents are dealt with in a prompt and appropriate manner.
- The Senior Leadership Team will receive regular monitoring reports from the Outside Agency.

IT Outsourced Agency

The agency will:

- Keep up to date with the latest risks to students whilst using technology, familiarise themselves with the latest research and available resources for college and home use.
- Review this guidance regularly and bring any matters to the attention of the Head of College.
- Advise the Head of College, AGC on all e-safety matters.
- Engage with the college community on e-safety matters at college and/or at home.
- Monitor inappropriate usage, alert and report any matters of concern to the relevant person, depending on severity.
- Ensure any technical e-safety measures in college (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Report termly to the Senior Leadership Team on matters arising.

Designated Safeguarding Lead

The designated safeguarding lead will be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- Access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- Online-bullying

The designated safeguarding lead is focusing on safeguarding issues and not technical issues arising.

All Students

The Student Acceptable Use guidance contains the boundaries of use for ICT equipment and services in this college. The S6C Student Disciplinary guidance is invoked when Deviation or misuse of ICT equipment or services occurs.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at college or outside of college.

Technology

Students can work in a safe and secure environment using the College's Google Workspace access via the s6c.mlp.college domain. All students and staff must use these safe channels to communicate and collaborate. This can be accessed from a BYOD laptop, tablet, computer or mobile phone.

Students can collaborate electronically in lessons or independent study via Google Meet or Google Chat to message or video call (video meetings can only be accessed when a member of staff is present). Students must not set up study groups using other social media platforms - the college system offers important safeguards. All students are able to access these apps, even if they choose to have limited access to a smartphone/ other apps/ social media and so the use of our college platforms is also fair and accessible. Our remote learning guidance is available on our website that explains the processes expected for students learning online at home.

1:1 sessions with staff should take place using college platforms.

Telephone contact:

Occasionally we may need to use a telephone to contact a student. Student mobile phone numbers are listed on Ed:gen and may be used if we are concerned about well being - all staff personal numbers will be withheld.

Online teaching and support meetings

If students are communicating with staff online, in a class, small group, 1:1 or in a support meeting, then we ask that students look at our guidance for safe and effective online learning.

Teachers will ask students to unmute their mics to contribute to online classes and support meetings.

Pastoral contact can be offered via messaging if a student is more comfortable with this.

Staff may ask students to put their cameras on during the discussion section of the lesson or a support meeting. This will allow the staff member to read the students' reactions, as we do in a classroom setting. Students are able to change their background before logging into Google Meet or whilst in Meet so that their privacy of their home is maintained. No student will be forced to turn on their camera - if they wish not to do so , then this will be respected.

Students should not be on simultaneous calls with others outside S6C during a college class, meeting or club.

Students should be up and dressed for online sessions, unless they are unwell, in which case they may wish to be off screen for any support meetings - this is important for safeguarding reasons but also for positive mental health and wellbeing.

S6C uses a range of devices including PC's, laptops, and Chromebooks. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

- **Internet Filtering:** we use software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites.

- **Email Filtering:** we use software that prevents any infected email to be sent from the college, or to be received by the college. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

- **Data Security:** No data is to leave the college on an unencrypted device. Staff and students will have access to data via the cloud and it is not necessary to use USB sticks or drives. Any breach (i.e. loss/theft of device such as laptop or storage device) is to be brought to the attention of the Head of College immediately. All staff laptops are encrypted.

- **Passwords:** all staff and students will be unable to access any device

without a unique username and password. The Outsourced agency will be responsible for ensuring that passwords change on a regular basis.

- **Anti-Virus:** All capable devices will have anti-virus software.

Safe Use

Internet

Use of the Internet in college is a privilege, not a right. The College network has a filtering and monitoring system in place to stop students and staff being exposed to identified risks

Email

Emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Use of personal email addresses for work purposes is not permitted.

Students are permitted to use the college email system, and as such will be given their own email address.

Photos and videos

- All parents must sign a photo/video release form as part of the enrollment pack.
- No students or staff should be photographed without their permission.
- No photos or video should be taken in classrooms without permission from the teacher.

Social Networking

There are many social networking services available; S6C is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider college community. The following social media services are permitted for use within S6C; should staff wish to use other social media, permission must first be sought via the Head of College for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in college.
- Twitter – used by the college as a broadcast service (see below).

- Facebook – used by the college as a broadcast service (see below).
- Instagram - used by the college as a broadcast service (see below).
- TikTok - used by the college as a broadcast service (see below).
- Snapchat - used by the college as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share college information with the wider college community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (recorded electronically) must be consulted before any image or video of any student is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the college are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and takedown guidance

Should it come to the college's attention that there is a resource which has been inadvertently uploaded, and the college does not have copyright permission to use that resource, it will be removed within one working day.

Incidents

Any e-safety incident (any breach of this guidance) is to be brought to the immediate attention of the Head of College and in their absence any member of SLT. The S6C Safeguarding guidance should then be followed and records will be recorded electronically in CPOMs. The views of the student/s will be listened to and assessed. If required the Student Disciplinary guidance will be activated.

Training and Curriculum

It is important that the wider college community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this

includes updated awareness of new and emerging issues. As such, S6C will have an annual programme of training, which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the college, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

Acceptable Use guidance – Staff

Note: All Internet and email activity is subject to monitoring

You must read this guidance in conjunction with the e-Safety guidance above.

Internet access

You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be reported as an e-incident to the Head of College.

Social networking

Social networking is allowed in college in accordance with the e-safety guidance only. Staff using social networking for personal use should never undermine or bring the college, staff, parents or students into disrepute. Staff should not become "friends" with parents or students on personal social networks.

Use of Email

Staff are not permitted to use college email addresses for personal business. All email should be kept professional. Staff are reminded that college data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords

Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff, student, or IT support agency.

Data Protection

If it is necessary for you to take work home, or off site, you should ensure that your device (laptop) is kept encrypted and secure. College data is stored in the cloud and staff will be able to access resources via Microsoft Office 365 or Google Apps for Education from home.

Personal Use of College ICT

You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head of College who will set the boundaries of personal use.

Images and Videos

You should not upload onto any internet site or service images or videos of yourself, other staff or students without consent. This is applicable professionally (in college) or personally (i.e. staff outings)

Use of Personal ICT

The college has a BYOD (bring your own device including mobile phones) guidance. Any personal ICT equipment used in college will be subject to the BYOD processes and controls.

Viruses and other malware

Any virus outbreaks are to be reported to the external outsources IT agency as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the persons involved.

E-Safety

Like health and safety, e-safety is the responsibility of everyone to everyone. As such, you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

Acceptable Use guidance – Students

Students are responsible for good behaviour on the Internet just as they are in a classroom. General college rules apply. The Internet is provided for students to conduct research and communicate with others in order to enhance learning. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. Users should not expect that files stored on the college network are private. College staff will, as a matter of course, monitor the way students are using ICT and any inappropriate usage will be dealt with under the college's disciplinary guidance.

Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Students will be expected to understand the guidance usage for mobile devices and digital cameras. Students should know and understand the guidance on the taking / use of images and online bullying.

Unacceptable use of the Network

Illegal Activities

- Sending or displaying offensive messages or pictures, to include the distribution of sexually explicit material
- Accessing, uploading, downloading or distributing pornographic material including consensual and non-consensual sharing of nude and semi-nude images or videos (also known as Sexting or youth produced sexual imagery)
- Any images obtained via Upskirting (taking a photo under someone's clothing usually without their knowledge with the intention of viewing genitals or buttocks with or without underwear)
- Violating copyright laws
- Accessing or downloading any material in violation of the law
- Unauthorised attempt to discover a computer password
- Hacking (unauthorised attempt to bypass security)
- Impersonation (the act of pretending to be someone else by setting up a false profile, or stealing someone's password with a view to posting false material that will endanger them, cause them distress or cause them to be falsely accused)

Inappropriate Language and Harassment in electronic communication

- Using vulgar or obscene language in any electronic communication
- Harassing, insulting, defaming, denigrating, or attacking others
- Spamming other users by sending unsolicited junk email (including chain letters)
- Cyber stalking including cyber bullying (cyber threats or blackmail using digital resources or text)
- Deliberately sharing someone's personal or sensitive information
- Using the college brand inappropriately on social media platforms

Endangering Personal Safety

- Revealing personal contact information (home address, telephone number, personal details, id numbers, etc.) to other individuals over the internet
- Arranging to meet people contacted over the internet without approval

Breaching System Security

- Intentionally spreading viruses, worms, chain letters, or Trojans
- Vandalising computers or peripheral equipment, computer systems or computer networks
- Altering, moving or deleting the files belonging to others
- Using another's password, or providing your password to another person
- Unauthorised attempt to access the network, including use of the network on someone else's login
- Attempting to access the network without providing assigned user name and password at the log-on screen
- Using any internet 'service' that attempts to 'mask' or 'hide' its identity from the college network security e.g. 'Tor' or 'proxy' sites. This includes personal VPN's
- Using 'SSH' services to 'tunnel' traffic through a firewall without permission from the Network Manager

Invading Privacy

- Trespassing in another's folders, work or files
- Reposting a message that was sent to you privately, without permission of the original Sender

Misuse of Limited Resources

- Posting unauthorised college related video or audio to public spaces, e.g. YouTube, Google Video, either as a 'member' of the service or anonymously
- Publishing any copyrighted materials provided to students in class to public

domain
● Plagiarising any work posted to social spaces as reference materials.
● Accessing games and personal entertainment sites not directly related to the area of study at time of access.

Parents / Carers

Parents/carers play a crucial role in ensuring that their young person understands the need to use the internet/mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues through communications on our website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the college in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at college events
- Access to parents' sections of the website/Google Classroom
- Their young person's personal devices in the college

Community Users

Community Users who access college systems or programmes as part of the wider college provision will be expected to adhere to this guidance.

Keeping Children Safe in Education 2023

This guidance has been updated to reflect changes in KCSIE 2023. Further guidance to support our young people and parents/carers about online safety can be found in this document.