E-Safety and ICT Acceptable Usage

Date of last review	September 2025
Date of next review	September 2026
Review period	Annual
Owner	Head of College

Statement

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

- Users: refers to staff, governing body, 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 or 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, governing body, parents

Safeguarding is a serious matter at S6C. The college uses 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 policy is reviewed on a regular basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this document 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 document is available for anybody to read on the S6C website.

Introduction

The online world is second nature to many of our students and the college respects their knowledge. However, 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 the non-consensual sharing of images.

The college encourages students to think very carefully about these issues and to read and think about the information shared, even if they feel they know how to keep themselves safe.

Keeping Children Safe in Education 2024

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
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm, for example making, sending and receiving explicit images and online bullying
- Commerce: risks such as online gambling, inappropriate advertising, phishing and financial scams

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 session 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 at any time in the Google Information Classroom. Information is also shared with parents and carers via the college's Weekly Update.

Governance: Roles and Responsibilities

Governing Body

The governing body is accountable for ensuring that the college has effective policies and procedures in place. The governing body will:

- Review this document periodically and in response to any e-safety incident, to ensure the document is up to date, covers all aspects of technology use within the college, that e-safety incidents were appropriately dealt with, and that the document was effective in managing those incidents
- Appoint one governor to have overall responsibility for the governance of e-safety at the college, who will: keep up to date with emerging risks and threats; receive regular updates from the Head of College regarding training, identified risks and any incidents; and report to governors at the Local Governing Body meetings

Head of College

Reporting to the MLP Director of Education, the Head of College has overall responsibility for e-safety within the college. The day-to-day management is delegated to an outside agency.

The Head of College will ensure that:

- Appropriate ICT training throughout the college is planned, up to date, and appropriate to the recipient
- The designated IT Support Agency has had appropriate CPD to undertake the day-to-day duties

- All e-safety incidents are dealt with in a prompt and appropriate manner
- The Senior Leadership Team receives 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 and familiarise themselves with the latest research and available resources
- Review this document regularly and bring any matters to the attention of the Head of College
- Advise the Head of College and governing body on all e-safety matters
- 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 or inappropriate materials
- Inappropriate online contact with adults or strangers
- Potential or actual incidents of grooming
- Online bullying

All students

The Student Acceptable Use document contains the boundaries of use for ICT equipment and services in this college. The S6C Student Disciplinary Policy is invoked when deviation or misuse of ICT equipment or services occurs. E-safety is embedded into the curriculum and students will be given the appropriate advice and guidance by staff.

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. 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, as the college system offers important safeguards.

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

Telephone contact

Occasionally the college may need to use a telephone to contact a student. Student mobile phone numbers are listed on Schoolpod and may be used if the college is concerned about a student's wellbeing. 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, students should follow the college's guidance for safe and effective online learning.

Teachers will ask students to unmute their microphones to contribute to online classes and support meetings. Staff may ask students to put their cameras on during the discussion section of a lesson or a support meeting. Students are able to change their background before logging into Google Meet to maintain the privacy of their home. No student will be forced to turn on their camera.

Students should not be on simultaneous calls with others outside S6C during a college class, meeting or club. Students should be up and dressed appropriately for online sessions as they would be in college.

Assistive technology in use

S6C uses a range of devices including PCs, laptops and Chromebooks. To safeguard the student and prevent loss of personal data, the following assistive technology is employed:

- Internet filtering: software that prevents unauthorised access to illegal or inappropriate websites
- Email filtering: software that prevents any infected email from being sent from or received by the college
- Data security: no data is to leave the college on an unencrypted device. Any breach (loss or theft of a device such as a laptop or storage device) must 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 is responsible for ensuring that passwords change on a regular basis
- Anti-virus: all capable devices will have anti-virus software
- Over-the-shoulder monitoring: all staff can and will view students' screens while in the classroom and report any inappropriate use to the safeguarding team

Safe Use

Internet

Use of the internet in college is a privilege, not a right. The college network has a filtering system in place to stop students and staff being exposed to identified risks. Monitoring is provided over the shoulder.

Email

Emails are subject to Freedom of Information requests. 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 will be given their own email address.

Photos and videos

- All parents must sign a photo/video release form as part of the enrolment 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

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: Blogging, Twitter/X, Facebook, Instagram, TikTok, Snapchat (all used as broadcast services only).

A broadcast service is a one-way communication method 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 must 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 or initials are to be used
- Where services are "comment enabled", comments are to be set to "moderated"
- All posted data must conform to copyright law

Notice and takedown

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 document) is to be brought to the immediate attention of the Head of College and, in their absence, any member of SLT. The S6C Safeguarding Policy should then be followed and records will be recorded electronically in CPOMs. The views of the student or students will be listened to and assessed. If required, the Student Disciplinary Policy will be activated.

Training and Curriculum

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. Further training or lessons will be established as necessary in response to any incidents.

Acceptable Use: Staff

> All internet and email activity is subject to monitoring. This section should be read in conjunction with the e-safety section above.

Internet access

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

Social networking

Social networking is allowed in college in accordance with the e-safety document 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 to take work home or off site, staff should ensure that their device 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

Staff 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

Staff should not upload onto any internet site or service, images or videos of themselves, other staff or students without consent. This applies professionally (in college) and personally (e.g. staff outings).

Use of personal ICT

The college uses BYOD (Bring Your Own Device, including mobile phones). 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 outsourced IT agency as soon as practical, along with the name of the virus (if known) and actions taken.

Acceptable Use: 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. Access is a privilege, not a right, and 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 policy.

Unacceptable use of the network

Illegal activities

- Sending or displaying offensive messages or pictures, including 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
- Any images obtained via upskirting
- Violating copyright laws
- Accessing or downloading any material in violation of the law
- Unauthorised attempt to discover a computer password
- Cracking or hacking (unauthorised attempt to bypass security)
- Impersonation (pretending to be someone else by setting up a false profile, or stealing someone's password)

Inappropriate language and harassment

- 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
- Using any internet service that attempts to mask or hide its identity from the college network security, e.g. Tor or proxy sites, including personal VPNs
- Using SSH services to tunnel traffic through a firewall without permission from the Head of College

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
- 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 and Carers

Parents and carers play a crucial role in ensuring that their young person understands the need to use the internet and mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues through communications on the website, social media and information about national/local online safety campaigns and 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 document.

Keeping Children Safe in Education 2024

This document has been updated to reflect changes in KCSIE 2024.