St. Columba's College

IT Acceptable Use and E-Safety Policy [Students]

This policy applies across the College at all age ranges including Early Years, Prep and Senior Schools. It should be read in conjunction with the Code of Conduct for Students and the Safeguarding Policy.

St. Columba’s College is conducted in the educational tradition of the Brothers of the Sacred Heart. The school environment is best described by the term “sanctuary,” a place where students sense the compassion which motivates those who care for them, where they feel safe to become the best person God created them to be.

Policy owner:	Deputy Head
Date reviewed:	January 2024
Date of next review:	January 2026
Ratify by governors:	No

Section 1 Application, Purpose and Scope

Each year, students will be asked to sign off on this policy. However, by signing into their network account, or using any College device, files or applications, students are by default agreeing to abide by this policy, even if they have not formally signed off.

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities, but also present new risks and challenges. This policy is designed to protect all users of College IT and to provide students with clear guidelines about the use of the technology, as part of our e-safety provision. The guidelines set out the individual's responsibility to ensure nothing is done that constitutes an abuse of the College network systems or resources, as well as information about keeping oneself safe online and showing respect to others whilst using IT.

The IT Acceptable Use policy covers not only physical property but also the College's intellectual property to include photographs of events, emails and school data on other personal mobile devices. It also covers the use of College issued devices, whether at home or at school.

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children. It should be read in conjunction with the Code of Conduct for Students, which provides a broader framework for student behaviour and expectations, and also links to the Safeguarding Policy. These documents may be found on the College website.

Section 2 Network Monitoring

Computer accounts are the property of the College and are designed to assist in the performance of schoolwork. The College has the right to monitor all aspects of use of any applications or systems that are made available for use by the College, and to intercept and record any communications made or received, including by telephone, email or other forms of Internet communications using College devices, accounts or networks.

The College reserves the right to use software or hardware devices to investigate where misuse is suspected and to counteract the circumvention of College security systems i.e. using a personal email account to transmit data.

The College uses a systematic, thorough and proactive approach to web filtering which seeks to protect students in school and educate for private usage at home. The College also closely monitors the use of the devices it provides, so as to ensure the principles of appropriate use and safeguarding particularly in reference to inappropriate and harmful searches, Child Sexual Exploitation, prevention of radicalisation and extremism and effectively all types of grooming on-line. However, as a fail-safe, if students do somehow encounter such material in school, they know that they must report the incident to the nearest teacher or the College's IT Services Team who will deal with it in line with school policy. Outside of school, students should also be aware that their school device is monitored and should not be used for any inappropriate purpose.

Section 3 Acceptable Use

The College IT facilities and systems may be used for lawful purposes only. Students are not allowed to create, store, distribute, transmit, or allow the creation, storage, distribution or transmission of any unlawful material whether intentionally or otherwise.

In signing into their network account, students agree not to access, create, send or receive materials or data which is deemed to be:

- In violation of any laws or regulation, a breach of any criminal legislation, other rights or has any fraudulent purpose or effect.
- Defamatory, offensive, abusive, indecent or obscene (i.e. pornography of any category). Disciplinary and / or civil action may arise if this is the case.
- Violent, or with the intent to incite a violent act.
- Constituting harassment.
- In breach of confidence, privacy or undermines the reputation of the College, its members or its ethos.
- In breach of any third-party intellectual property rights i.e. copyright. It is prohibited to post, upload or distribute or permit the posting or distributing of copyrighted material on the College servers without the copyright holder’s consent.
- In breach of any College rule, for example photos or footage taken in school without the express permission of a member of staff
- Violating or compromising any aspect of the System Network Security i.e.
    - Circumventing network access control
    - Unauthorised access to or use of data, systems or networks, including attempts to monitor the data traffic or probe, scan or test the vulnerability of a system or network, without express authorisation from the Head or Deputy.

  - Interfering with any user account, workstation, host or network to reduce its proper functioning or deliberate attempts to degrade or deny access to the system.

Any breaches of the above will lead to sanctions in line with the Code of Conduct and Behaviour policy, including potentially the permanent withdrawal of IT use in the College.

Section 4 Responsible Use

When using a computer, students must:

- Not interfere with the software or hardware configurations of networked equipment or systems.
- Not install, download or use any additional software on the College network (e.g.: wallpaper, screen savers, games, peer to peer applications – these are examples and do not constitute an exhaustive list).
- Not link any personal computing device to the College network without consulting IT Services and observing the wireless access guidelines.
- Never knowingly introduce viruses or other disruptive elements to the College network.
- Avoid using portable storage devices. Students should save and share files via the OneDrive cloud storage system, which can be accessed from any device at any time. When the use of portable devices is necessary, it must be sanctioned by the monitoring staff member. Antivirus software will automatically screen such devices.
- Not reveal personal details or those of others online (addresses, contact numbers etc.) or arrange to meet someone outside of school via the College network.
- Change their password to a personal one the first time they login, and regularly thereafter. Passwords must be a minimum of 8 characters long and contain a capital letter and a number. It cannot contain any part of their name (local rules apply in Prep). Passwords must be kept secure, i.e. not shared.
- Log off the computer at the end of a session and do not leave it unattended even for a short time if their account is open.
- Never use an account belonging to another user or guess or steal another's password.
- Not corrupt, destroy, disrupt or violate the privacy of another user's data or work.
- Not use or interfere with other students' equipment (e.g. using their keyboard, mouse or turning off their device at the power button).

- Not do anything which could be considered negligent or harmful with regard to their device or the network.

Section 5 Device Protocols

While at the College, students will be loaned a device pack, which includes the following equipment:

- Microsoft Surface Pro
- Microsoft Surface Pro Keyboard and Classroom Stylus
- Surface Pro Case
- Surface Pro Charger
- Battery Pack & USB-C Cable (Senior Students)

Students must take good care of this equipment. If any of the equipment issued to a student develops a fault or is lost, this must be reported to IT services as soon as possible.

Expectations with regards to the use of device are as follows:

- arrive at school with the device fully charged;
- put the device on the desk in the ‘devices closed’ position at the start of the lesson;
- listen to and act on teacher instructions on use of the device in lessons;
- do not eat or drink when using the device;
- always keep the device in its protective case;
- bring in your device, pen, keyboard cover and stylus pen every day;
- all device related items are named (items listed above);
- the device and related items must be handled and stored with care, so ensure the device is placed in your bag at the end of every lesson and when not in use;
- ensure notifications are off in lesson;
- no use of VPNs or downloading of unauthorised content and applications;

- electronic communications between other students and staff are positive, constructive, and collaborative;

- headphones should only be used for learning purposes and with the direct permission of the teacher.

It is the student's responsibility to charge their devices each evening. If they arrive at school with their device not charged and without their battery pack, they will be directed to ICT Services from where they can borrow a battery pack. 2x ‘device not charged’ points in one week will result in a lunchtime detention.

Minor behaviour infractions related to device misuse will result in a distraction/ disruption point on SIMS (akin to consequence 2 of the behaviour ladder). 3 such points in a week will result in an after-school detention. Such infractions include, but are not limited to, visiting irrelevant websites, turning off or tampering with another student’s device, messaging other students, playing games, being on the device when the teacher has not authorised it or completing homework for another lesson.

The filming of any part of the lesson or of other students in school is strictly forbidden and will result in a more serious sanction. This also includes taking photos of others in the room or recording voices including that of the teacher. These more serious incidents will be dealt with on a case-by-case basis, but the minimum sanction awarded will be a Saturday detention.

Any short-term exceptions to this rule, such as the filming of a short play in Drama for the purpose of analysis, will be explained fully by the teacher and will be done under limited and time-framed parameters.

Repeated misuse of the device will result in a ban.

When at school, devices must only be used in a classroom, the library or the Sixth Form Centre. Students must not use their devices at breaktimes or lunchtimes, unless as part of a supervised activity. No students should be using their device on the playground, as it may get damaged.

Students must take a reasonable amount of care of any device being used, being careful to keep it away from unnecessary physical contact and scenarios, away from liquids, ensuring it is stored safely and protectively both on the school site, at home and in transit to and from school (in the context of a school leased device).

The development of artificial intelligence (AI) tools has increased rapidly in recent years, and AI-based applications such as ChatGPT are a valuable learning aid. However, students must ensure that they understand the risks and limitations of AI, and the ethical issues that these technologies can create, especially in relation to the use of copyrighted materials, and the risks of plagiarism, when using AI to generate content.

As a general rule, it is assumed that students are not allowed to use AI in their work. However, in certain tasks, your teacher will allow you to make some use of AI, based on the "Traffic Light System". Where this is the case, staff will confirm the level of AI use at the start of each task:

Traffic Light Indication	**AI Application**	**Guidelines**	**Example Tasks**
Green Signal	AI use allowed	You can use AI but remember to reference all your sources. Review all content for accuracy and bias.	e.g., Some research projects, multimedia presentations, discursive essays
Yellow Signal	Limited AI use	AI can assist you with suggestions and guidance, but the work you submit should be your own. Verify all AI-generated content for accuracy.	e.g., Debates, narrative creation, business proposals
Red Signal	AI use prohibited	In tasks, exams and assessments designed to assess your foundational skills, you shouldn't use AI.	e.g., Handwritten compositions, in-class quizzes, laboratory reports

Section 6 Classroom Use Protocols

When in a computer room, or while using devices in a normal classroom:

- Equipment must only be used at appropriate times, and always in accordance with the teacher's instructions. Students must listen to all instructions relating to the use of their devices and may not access any websites or applications that do not form part of the lesson.
- Students are not permitted to attempt to solve technical problems with IT equipment: this must be done by IT Services only.
- Students should not remove or change keyboards, mice and cables from any piece of equipment. They should ask the teacher or IT services for a replacement if their equipment is faulty.

Section 7 Internet Use

Students are responsible for their Internet browsing, accounts and the content of communications using the College e-safe systems. In school, searches must be related to their research and learning as directed by staff and limited to school related investigation or communications. Access to sites will be allowed only to those given approval. Content of web pages or web searches are dynamically filtered for unsuitable words and images. Access to public unmoderated chat rooms and the use of social networking sites is prohibited in the College (local rules apply to Sixth Form). Never make or post defamatory or offensive material or comments of any nature in communications irrespective of whether they are intended to cause offence or not.

Students must not research materials (unless as part of a legitimate study directed by staff) which may promote ideologies and practices contravening British Values, thereby undermining the safeguards undertaken by the UK Government to prevent extremism and radicalization (reference: CONTEST (The UK Government Strategy for Countering the Terrorist Threat July 2011) and PREVENT Strategy (the aim of which is to stop individuals becoming allied to and active in terrorism). Concerns over such matters are bound by the Safeguarding principles and practices of the school and are to be shared with the Designated Safeguarding Leads.

Section 8 Communications

All communications between students and staff, and peer to peer communications must be conducted through the school-based accounts.

Staff and students are never to share private email or social media accounts. This remains the case when in any communication between school and home.

The College uses Microsoft Teams to share lesson content, homework, announcements and information. Students must not use Teams in a disruptive or inappropriate manner, e.g., reacting to or commenting on posts unnecessarily or sending messages to a class or group of students via a Teams channel. Use of messaging and chat in Microsoft Teams must be relevant, appropriate, used for the purposes of learning and respectful in tone. It may sometimes be appropriate for students to raise a question with a teacher via Teams, but most staff-student communication is expected to take place through other methods (e.g. in class or via e-mail).

The College provides a secure e-mail system for students to use. When using this system, students must adhere to the following rules:

- manage their personal email box to limit its size, deleting emails once redundant;
- never forward mail to anyone inside or outside the College for whom the information contained could be regarded as inappropriate;
- Never mail large groups of staff or students with messages that are not on College business.
- never mail any student or group of students a message which contains bullying or abusive comments about another person;
- Ensure that any outside communications would not involve the College in a potentially awkward or defamatory situation.
- never open attachments unless sure of the source and ensure that the content conforms to Internet protocols.

It is forbidden to distribute chain letters. Suspicious messages are to be reported to IT Services and then deleted and not forwarded.

Section 9 Other Mobile Communications Protocols

Given that all Senior and Upper Prep students now have their own device available for learning purposes in school, they are not permitted to use mobile phones during school time, unless they need to contact home urgently. If the latter, this is only allowed with the express permission of Reception staff and is to take place in the Reception area (local rules apply in the 6th Form Centre). Any attempt to use a phone elsewhere or at any other time will result in a warning and negative point being awarded. On a second occasion, the phone will be confiscated by the Deputy Head and retained overnight. Any subsequent breaches of this rule will lead to that student not being allowed to bring their phone to school. The sending of text or social media messages during the school day is forbidden. The creation of Mobile Hotspots is always forbidden in the College.

Personal gaming consoles are not permitted in school for any year group unless for specific use as part of the EECA provision. Personal laptops / computers are only permitted for 6th Form students until the school devices are available to all, or where IT services or SEND department give express permission.

Section 10 Protocol in the event of damage, theft, loss or child leaving the College

Any damage, theft, or loss much be reported immediately to a member of the IT Services department. All insurance claims will be processed by IT Services, theft-based claims must be accompanied by a police reference number, however lost devices are not covered. Should a student lose a device this must be reported immediately and the College will make contact with parents regarding the next steps to replace the device. Keyboard, pens, and cases are covered by their standard warranty and any lost items will be billed at the current market price.
When a device is sent off for repair, or a replacement is required, students will be issued with a temporary replacement device. Whilst we aim to equip students with a like for like replacement device this may not always be possible due to stock levels and numbers of devices out for repair at the time.

If your child leaves the College, you will be expected to settle your school accounts and return the device and any associated accessories issued to your child with the device. When this has occurred, your original school deposit will be released back to you net of any deductions made in accordance with the relevant sections of the Parent Contract in force at the time.
If your child leaves midway through the three-year lease (e.g. your child started the lease in Form 4 and does not return/goes elsewhere for Sixth Form or leaves in Form 2 or 3 for another school) you are not liable for device payments beyond leaving the College. As long as your account is settled for time spent at the College, no obligation to finish the cost of the lease exists.