St. Columba's College

ICT 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:	KMA
Date reviewed:	July 2020
Date of next review:	July 2023
Ratify by governors:	No

Section 1 Application, Purpose and Scope

By signing into their network account, students are agreeing to abide by this policy.

This policy is designed to protect all users of the College ICT 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 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 ICT Acceptable Use policy covers not only our physical property but also the College's intellectual property to include photographs of events, emails and school data on other personal mobile devices.

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children. We recognize that the online world provides many opportunities; however, it can also present risks and challenges. 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.

Section 2 Network Monitoring

Computer accounts are the property of the College and are designed to assist in the performance of school work. The College has the right to monitor all aspects of use within its Information and Computer Technology telecommunication systems that are made available for use, to intercept and record any communications made or received, including by telephone, email or other forms of Internet communications.

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

The College uses a systematic approach to web filtering which seeks to protect students from the above in school and so educate for private usage at home. The College also seeks to monitor the use of ICT resources and the Internet, so as to ensure the principles of appropriate use and safeguarding particularly in reference to Child Sexual Exploitation, prevention of radicalization 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 will know that they should report the incident to the nearest teacher or the College's IT Services Team which will deal with it according to the school AUP.

Section 3 Acceptable Use

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

In signing into their network account, students agree not to 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.
- 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 his/her 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, 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 (i.e. screen savers, games, peer to peer applications).
- Not link any personal computing device to the Network without consulting IT Services and observe the wireless access guidelines.
- Never knowingly introduce viruses or other disruptive elements to the Network.
- Only use portable storage devices when 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.
- Not take drinks or food into the IT Suites.
- Change their password to a personal one the first time they login. It 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 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' hardware/software equipment (e.g. using their keyboard, mouse or turning off their PC at the power button).

Section 5 Classroom Use Protocols

- All equipment in the classroom should only be used under direct supervision of and at the request of a member of staff.
- Students are not permitted to attempt to solve problems with IT equipment: this must be done by IT Services only.
- Cables are not to be removed or changed over on any IT Equipment.
- Personal laptops / computers or gaming consoles are not permitted unless permission is given for individuals or year groups for BYOD.
- Students should not remove/change keyboards/mice from un-used PCs. They should ask the teacher or IT services for a replacement if their equipment is faulty.

Section 6 Internet Use

Students are responsible for their Internet browsing, accounts and the content of communications using the College e-safe systems. 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 such as Twitter (local rules apply to Sixth Form), Facebook, etc. 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 7 Email Use

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 accounts. This remains the case when in any communication between school and home.

Students must:

- Manage their personal email box to limit its size, deleting emails once redundant.
- Not 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.
- 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. Spam messages are to be deleted and not forwarded.

Section 8 Other mobile communications protocols

Students are not permitted to use mobile devices during lessons or during formal school time, unless they are part of the BYOD rollout or given express permission to do so.

Mobile phone use is not permitted unless permission is sought through Reception. All calls are to be made in the Reception area and only after permission has been granted (local rules apply for Sixth Form). The sending of text messages during the school day is forbidden. The creation of Mobile Hotspots is forbidden in the College at all time.