

Bring Your Own Device (BYOD) Code of Conduct



St Columba
College

Contents

1. Bring Your Own Device (BYOD) Code of Conduct.....	3
2. Acceptable Devices & Minimum Specifications	3
3. Network and Internet Access.....	3
4. Powering Devices	3
5. Technical Support.....	3
6. Care, Insurance and Liability.....	3
7. Content	4
8. Responsible Use	4
Equipment.....	4
Network.....	4
Acceptable equipment access and use.....	4
Intellectual Property and Copyright.....	4
Privacy, Security and Confidentiality.....	4
Misuse and Breaches of Acceptable Use.....	5

Policy Title	Bring Your Own Device Code of Conduct
Ratified by Leadership	October 2023
Date Due For Review	Reviewed after 2 years or before if required.

1. Bring Your Own Device (BYOD) Code of Conduct

Use of the internet and digital technologies provides great educational benefits to students. Digital devices have the potential to encourage student critical thinking, problem solving, communication, collaboration and research skills and prepare students for a digital world beyond school. Bring Your Own Device (BYOD) and school access to these technologies is facilitated with the expectation that students will act in a considerate, safe and responsible manner. Prior to students accessing St Columba digital resources, students and parents/caregivers are required to read and agree to the 'Bring Your Own Device Code of Conduct.'

In connecting to the College's Wi-Fi, students will have access to the internet, email, storage and SEQTA facilities that will provide effective communication between students and teachers, facilitating the transfer of instruction and student work. These digital resources are provided by the College and are to be used responsibly to save and store resources and evidence of learning. ICT staff may review users' files and communications to maintain system integrity. Digital devices (student owned and College facilities) are to be used for learning purposes only.

2. Acceptable Devices & Minimum Specifications

- Windows device (please refer to BYOD Device Specification document for device requirements).
 - Please note that Android tablets, MacBook's, Chromebooks, Apple iPads, and Windows S mode are not suitable for BYOD.
- BYOD devices are not to be shared.

3. Network and Internet Access

- Devices will not be physically networked. Content will only be accessed through the College Wi-Fi and will be subject to monitoring and filtering.
- Internet and online communication can be audited and traced to a specific user account.

4. Powering Devices

- Devices must be fully charged before they are brought to the College.

5. Technical Support

- BYOD laptops are not owned or managed by the College. The College will not offer any technical support relating to the device or its operation, other than assistance with connecting to the College Wi-Fi and related services.

6. Care, Insurance and Liability

- Students are responsible for the care of their devices.
- Devices must be clearly labelled for identification.
- A padded bag or protective sleeve should be used to reduce the risk of damage.
- Devices are to be secured in lockers when not in use i.e. recess and lunch (unless used for study purposes and under supervision) and lessons when they are not required.
- Devices are to be taken home at the end of the day.
- Care of device
 - Parents are responsible for insuring their child's device for loss, theft or damage.
 - The College accepts no responsibility for the loss or damage of any personal device.
 - The College will investigate any theft incident and normal discipline procedures will apply.

7. Content

- All content must remain appropriate, as deemed by the College, at all times.
- Parents/caregivers must ensure that all content stored on devices used in the College is compliant with copyright law and regulations.
- Parents/caregivers must ensure that devices used in school have virus-protection software installed that automatically downloads the latest anti-virus updates.

8. Responsible Use

Equipment

- Bring their device fully charged every school day.
- Use all equipment, resources and services responsibly and with care.

Network

- Use the wireless network and technologies provided by the College only for educational purposes. If an inappropriate site is accessed unintentionally then it should be closed, and the student should notify the teacher immediately. Under no circumstances is such material to be forwarded, downloaded or printed.
- Only use the College's Wi-Fi when at school. Mobile phone hot spotting and/or accessing a VPN for the purpose of gaining unfiltered internet access is strictly forbidden.

Acceptable equipment access and use

- Use their device during the school day *only* when granted permission to do so by the subject/study teacher in support of the learning program.
- Turn off devices during recess and lunch to preserve battery life. At these times, devices must be securely stored in lockers.
- Maintain respect for all individuals and therefore never use technology in ways that can offend, cause distress or intimidate others.
- Engage in safe, ethical and respectful on-line behaviour.
- Store college related files on Microsoft OneDrive, provided to each student free of charge.

The College is not responsible for any damages an individual may incur through the loss of data resulting from corrupted files or USBs, delays, non-deliveries, miss-deliveries, or service interruptions.

- Abide by the rule that digital devices are to be used solely for educational purposes to support learning programs. Social networking sites must not be accessed during College hours or on College premises.
- Not create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

Intellectual Property and Copyright

- Acknowledge all sources used in the production of work and therefore avoid infringement of copyright laws.

Privacy, Security and Confidentiality

- Respect the privacy of others when using digital technologies and refrain from revealing or using the personal details of any person without their permission.
- Abide by the rule that recording, filming, photographing, storing and/or transmitting images of others to any social media site or other form of publication is a serious offence which breaches privacy laws and will be treated as such.
- Use email responsibly and with care, and not open attachments from unknown sources, as they may contain viruses/malware.

- Never knowingly initiate or forward emails or other messages
 - A message that was sent in confidence
 - Chain letters and hoax emails
 - Spam, e.g., unsolicited advertising material
- Ensure that any images or material stored on devices are appropriate to the College environment and are used safely and responsibly in support of teaching and learning programs.
- Keep passwords confidential, and change them when prompted, or when known by another user.

Misuse and Breaches of Acceptable Use

Standard school discipline rules apply for misuse of the device contrary to the BYOD Code of Conduct. Students need to be aware that they will be held responsible while using St Columba's ICT facilities. Examples of action the school may take in cases of misuse include:

- The device is taken away by a teacher for the remainder of the lesson.
- The device is taken away by a House Leader or Deputy Principal for the remainder of the school day and/or until a parent or carer picks up the device.
- Removal of network and internet access.
- Conventional discipline procedures, including suspension or detention.

Please note: The Code of Conduct Agreement will be sent out electronically at the commencement of the school year for students and parents/caregivers to acknowledge and sign.