STUDENT DIGITAL CITIZENSHIP POLICY

Introduction

St Columba's College aims to embed a digital learning culture with clear policies and guidelines, in line with our Vision and Mission Statement and Values. The aim of the policy is to provide guidance to staff, students, parents/carers, and others in the community about what constitutes a safe, respectful and caring environment where technologies are used safely and responsibly for learning and communicating. This is in keeping with the College's Vision and Values, our legislative and professional obligations, and community expectations.

Purpose and Objectives

St Columba's College uses the internet and digital technologies as resources for learning and teaching tools. We view the internet and digital technologies as valuable resources for students and teachers.

At St Columba's College we:

- Have an approach to digital citizenship that incorporates our school's vision of guiding faith-filled discernment and empowering learners who are compelled to action, in our hope for a just world
- Have learning programs in place to educate our students to be safe and responsible users of digital technologies
- Supervise and support students using digital technologies for school-directed learning
- Use clear protocols and procedures to protect students working in online spaces. This includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at the earliest opportunity, and monitoring of network traffic/usage of College network infrastructure
- Provide a filtered internet service to block inappropriate content. We acknowledge, however, that full protection from inappropriate content cannot be guaranteed
- Use online sites and digital tools that support students' learning; specifically, Google Workspace for Education, Microsoft 365 and the SEQTA LMS for learning and assessment delivery
- Address issues or incidents that have the potential to impact on the wellbeing of our students and staff
- Refer suspected illegal online acts to the relevant Law Enforcement authority for investigation
- Support parents/carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home.

Policy

Student Expectations

Responsible Use

When using St Columba's Internet Access, Networks, Software and Hardware (including through the Device Program):

- Students will use all technological resources provided by the College (including access to the internet, or that utilise the College's network/s, responsibly and for educational purposes only
- Students will use the appropriate system when borrowing school laptops or iPads and return these items by the end of the school day on which they have been borrowed
- Students will not use a VPN to bypass the school internet filtering system
- Students must not encourage, participate or otherwise knowingly support others in prohibited use of College, or privately owned communication technologies, on the College site or at any College related activity
- Students will, when handling ICT devices, use care and notify a teacher of any damage or attention required to College owned ICT equipment.

When accessing information online:

- Students will respect copyright laws and intellectual property rights when using digital resources for academic or creative purposes (Refer to the Academic Honesty Policy)
- Students will properly attribute all sources used in their work and seek permission when necessary
- Students will abide by the terms and conditions for all online platforms/sites/services
- Students will not submit work as their own that has been created using AI technologies, unless directed by a teacher.

When using personal mobile phone/technology:

- Students will only utilise this technology outside of school hours (8.35 am – 3.00 pm), unless directed by the teacher for educational purposes
- Students will not engage in personal attacks, harass another person, bully others, or post private information about another person using SMS messages, phone calls or via any other means
- Students will not circulate any images that make reference and/or identify community members without their consent
- Students will not circulate or view explicit images. Children under the age of 18 are unable to give consent to these types of images
- Students acknowledge that mobile phones/devices are brought to school at their owner's risk. The College does not hold insurance for personal property brought to school and will not pay for any loss or damage to such property
- Students accept that mobile phones/devices being used in contravention of College policy may be confiscated and returned to parent/carer at a mutually agreed appointment time.

Respectful Use

- Students will maintain respectful and courteous communication with teachers, staff and fellow students when using the College's communication technologies, such as email, messaging platforms, or virtual collaboration tools

- Students will communicate professionally, constructively, and free from any form of harassment, discrimination, or cyberbullying
- Students will use educational networking sites such as, but not limited to, SEQTA Courses and Assessments, Google Workspace for Education, Microsoft 365 and SEQTA Direqt Messaging for educational purposes only
- Students will not create or disseminate any inappropriate, harmful or unsafe content online
- Students will report any inappropriate, harmful, or unsafe content online to a teacher, staff member, or the designated authority promptly, including any instances of cyberbullying, harassment, or other digital misconduct
- Students will only take and share photographs or sound or video recordings when others are aware the recording is taking place and have provided their explicit consent as part of an approved lesson
- Students and parents/carers acknowledge that while after school use of communication technologies by students is the responsibility of parents/carers, College policy requires that no student attending the College may identify, discuss, photograph or otherwise publish personal information or personal opinions about College community members, including staff and fellow students of the College.

Cyber Security and Safe Use

- Cyber Security is the responsibility of the entire College community and cyber criminals may target student email accounts to gain a foothold into the College network
- Students must be wary of phishing emails, these are emails that appear safe but have malicious intent. Students should err on the side of caution and delete them if they are unsure of their legitimacy. Students must only respond to emails that they are expecting and from sources known to them
- Students will protect their privacy rights and those of other students and staff by not giving out personal details including login details, full names, telephone numbers, addresses, images and passwords either online or in person
- Students will abide by network security requirements including; neither sharing user names or passwords with others; nor logging in to the College network with the sign in credentials of another student or staff member
- Students will seek to understand the terms and conditions of websites and online communities and be aware that content uploaded, or posted contributes to the student's digital footprint
- Students will strive to create a positive digital footprint for themselves and others, by thinking carefully about the content they upload or post online, knowing that this is a personal reflection of who they are and can influence what people think of them
- When online, students must not interact with posts that are in breach of the College's community expectations, this includes but is not limited to; hate speech or discriminatory language; harassment or cyberbullying; inappropriate or explicit material; violent or threatening content; false or defamatory statements about individuals or the College; any other content deemed to negatively impact relationships within the College community.

The Student Digital Citizenship Policy also applies during school excursions, camps, extra-curricular and remote learning contexts.

Breaches of Expectations

Breaches of any of the above expectations may result in consequences, as per the Student Management Guidelines. In some cases, these may also be reportable to authorities (ie Police, eSafety Commissioner).

Monitoring by the College

The College, as the licensee of Google Workspace for Education, Microsoft 365, SEQTA, and other online platforms, as the owner and provider of the network infrastructure, has the right and responsibility to check work or data on the College's networks, email platforms, internet traffic pathways, and other College ICT equipment/devices, without obtaining prior consent from the student.

- The College will, on occasion as required, analyse and monitor traffic via any/all internet protocols to help maintain an efficient and safe learning environment
- The College will restrict student access to certain sites and data for student protection from inappropriate content, but due to the nature of the internet full protection can never be guaranteed despite software and education programs that are put in place.

Related Policies and Procedures

- Digital Citizenship Staff Policy
- Bullying Prevention and Intervention Policy
- Child Safe Policy
- Academic Honesty Policy

Related Forms and Documents

- Student Management Guidelines
- Student Use of Mobile Phones (see Student Management Guidelines)
- Laptop Program Handbook

POLICY HISTORY AND SCHEDULE

Date of Approval:	October 2023
Approval Authority:	College Leadership Team
Delegated Contact Person:	Deputy Principal
Next Review Date:	October 2025