St Columba's Primary School, Wilston

ACCEPTABLE USE OF DEVICES AND DIGITAL RESOURCES CONSENT

Devices and digital resources, including access to and use of the internet and email, have become of critical importance to schools in the provision of innovative educational programs.

Brisbane Catholic Education and **St Columba's Primary School** are committed to educating students about safe internet and email practices and lawful and ethical online behaviour. Students will receive age-appropriate guidance and training to support responsible digital citizenship and navigate digital environments safely.

This document outlines responsibilities to ensure safe and secure ICT use, per Brisbane Catholic Education's standards for ethical, legal, and responsible use.

These responsibilities apply to all **St Columba's Primary School** technology resources, whether accessed via school-owned or personal devices, whether they remain on school grounds or are taken off the school grounds with permission from the school. **Technology resources are provided to students for educational purposes only. St Columba's Primary School** has specific guidelines relating to the use of technology, which are outlined below.

Each student and their Parent/Legal Guardian must sign the acknowledgment to confirm that they understand the requirements of acceptable use and the potential consequences of a breach of the responsibilities listed below.

Responsibilities of the School and Brisbane Catholic Education

Brisbane Catholic Education and **St Columba's Primary School** are committed to providing a safe, secure, and supportive digital learning environment. BCE and the school take the following actions to support the ethical, legal, and responsible use of technology resources by students.

a. **Filtered Internet Access**: BCE provides secure and filtered internet access on school grounds. Internet traffic is routed through Secure Web Gateway (SWG) devices that inspect and apply filtering policies to block inappropriate content. Filtered internet access does not apply when the student is using a school-owned device off-site.
b. **Device Management**: School-owned devices are configured with firewalls and management tools. BCE uses Mobile Device Management (MDM) solutions to set up, configure and manage student devices.
c. **Monitoring and Oversight**: BCE may monitor student use of enterprise platforms—including internet, email, messaging tools, and AI interactions—to identify non-compliance with acceptable use standards and protect system integrity and security. Schools may inspect or provide copies of communications when required by law or as part of investigations.

d. **Digital Citizenship Education**: Schools provide age-appropriate guidance and training to support responsible digital citizenship and safe online behaviour. Online safety education is incorporated in multiple curriculum areas.
e. **Use of Generative Artificial Intelligence Tools**: Brisbane Catholic Education and its schools acknowledge the evolving role of generative artificial intelligence (AI) in education. These technologies may be used to support curriculum planning, instructional delivery, and professional decision making, and by students to engage with AI systems under appropriate supervision. Use of Microsoft Copilot is logged and monitored by BCE to ensure compliance with acceptable use standards and to protect student safety and well-being. All use of generative AI—whether BCE-provisioned or individually accessed—must align with BCE's commitment to ethical, legal, and responsible technology use. This includes transparency in usage, safeguarding privacy and data, and ensuring that AI tools are used in ways that promote equity, inclusion, and human-centred learning.
f. **Support Services**: Schools have access to BCE IT support staff and services to assist with technical issues and ensure devices function effectively for learning.
g. **Acceptable Use Agreements**: BCE and schools require students and parents to sign annual ICT Acceptable Use Agreements to reinforce shared expectations and responsibilities.
h. **School-Based Policies and Plans**: Each school develops and implements local ICT operational plans and policies tailored to their community, including device usage guidelines and behaviour management strategies.
i. **Parent Engagement and Communication**: Schools provide information sessions and resources to help parents/guardians understand and manage technology use at home, including guidance on content filtering and supervision.
j. **Privacy and Data Protection**: BCE and the school take reasonable steps to protect student data. However, some services may store data on servers outside Australia, and while BCE aims to prevent unauthorised disclosures, it cannot control third-party breaches.

Responsibilities of Students

Permitted use of technology resources

1. Students must only access **St Columba's Primary School** technology resources for schoolwork. They must adhere to the school's guidance and instructions for the appropriate use of digital resources, including managing identified privacy risks.

   Appropriate use by a student
   a. complete class work set by teachers
   b. apply digital literacy skills
   c. conduct research for school activities
   d. communicate or collaborate with other students, teachers or experts in relation to schoolwork
   e. engage with digital tools in a respectful and responsible manner, ensuring all communication and content shared reflects the values of the school community.

Inappropriate use by a student

a. access or enter online communication outside of school-authorised platforms
b. access, post or send inappropriate digital content. This includes but is not limited to; content that is illegal, dangerous, obscene, offensive or could be considered bullying or harassment
c. access, share, solicit, or store material that breaches community standards, including child sexual exploitation, pro-terror content, extreme violence, drug-related material, or content related to cyberbullying, self-harm, school violence, hate speech, gambling, profanity, or adult content
d. commit plagiarism or violate copyright laws
e. download, install or use unauthorised computer applications
f. deliberately install viruses or other malware
g. use technology to attack or compromise another system or network
h. bypass the BCE network controls by any means, including utilising virtual private networks (VPN) or using a mobile hotspot

Use of Generative Artificial Intelligence (AI) Tools

2. Students must not enter personal, sensitive, or confidential information into AI tools (such as Copilot) except as required for approved learning activities.

3. Students must not use AI tools to generate or share personal, sensitive, or confidential information about themselves or others.
4. Students must use AI tools in accordance with the school's guidance and the BCE Acceptable Use Policy.

Privacy and Cybersafety

5. Students should understand that anything they post online — including on social media — is public, searchable, and may have lasting personal and community impacts. Their digital footprint reflects on themselves and the school.

6. For the safety of students, personal information about themselves or others should not be published publicly. For example, students should not post or share their own or anyone else's image, address, phone number or other personal details online.

7. Students should be cautious about interacting with AI personas or other online profiles, as they may not always represent real individuals or trusted sources. Students must not arrange to meet persons who they have met online.

8. Students should be aware that Brisbane Catholic Education monitors student use of enterprise platforms, including internet, email, messaging tools, and AI interactions, to ensure compliance with acceptable use standards. Where concerning or inappropriate behaviour is identified, the school will

be informed and may take appropriate action pursuant to the Student Code of Conduct. Additionally, the school may be required to inspect or provide copies of electronic communications where required by law or as part of an investigation into possible misuse of technology resources.

9. Students should be aware that 'Cloud' based tools and services are used for data storage and learning opportunities. Some of these services may store data on servers located outside Australia.

Cyberbullying and defamation

10. Students are prohibited from using digital or online tools to communicate or publish derogatory, impolite, or unkind remarks about others, or to send threatening, harassing, or offensive messages. Improper use of digital platforms and resources may result in defamation and be referred to legal authorities.

Security

11. Students are required to regularly update their devices to maintain security.

12. Students must use a secure password or passphrase and keep their username and password and personal information private. The password should be changed regularly in line with the Australian Curriculum and should be difficult for other people to guess. Students should take steps to ensure their device is inaccessible to others when unattended, e.g., lock screen.

13. Students must not use another person's name and password to access resources.

14. Students must report a suspected breach of security to the school and parent/guardian. Examples of a suspected breach include, but are not limited to, a virus being installed on the device or the student's password being shared with others.

Copyright

15. The use of material from the internet may be a breach of copyright or other intellectual property rights. Students must not use **St Columba's Primary School** technology resources to copy, download, store or transmit any such material that may include music, images, videos or any other form of media.

<u>Consequences following a breach of this Acceptable Use Statement</u>

1. A breach of this statement will be taken seriously and may result in disciplinary action.

2. Examples of possible consequences range from
    - **i. Temporary loss of device access**

i. The student's iPad/laptop is **confiscated for a set period** (e.g. the remainder of the lesson, the day, or several days).
ii. During this time, work is completed using **non-digital alternatives**.
iii. This reinforces that device use is a **privilege**, not an entitlement.

ii. Restricted use / supervised use

a. The student may:
   i. Use the device **only at school**, or
   ii. Use it **only under direct teacher supervision**, or
   iii. have specific apps, functions, or internet access **temporarily restricted**.
b. This is particularly appropriate where the misuse is ongoing but not severe.

iii. Device not permitted to be taken home

a. The device remains at school for a defined period.
b. This consequence:
   i. Reduces opportunities for further misuse,
   ii. Signals seriousness, and
   iii. Often involves **parent awareness and partnership** without escalating to Formal behaviour processes.

iv. Restorative action + parent notification

i. The student completes a reflection task (written or verbal) addressing:
ii. What BCE expectations were not met,
iii. The impact of their actions, and
iv. How they will use the device responsibly moving forward.
v. Parents/carers are informed, and expectations are clearly reset.
vi. This is especially effective for repeated breaches.

3. ***Students and Parents/Legal Guardians may be financially liable for damage caused to resources. Parents/Legal Guardians will be responsible for replacing (with genuine replacements) the loss of devices or other items related to the device provided by the school – such as charging cables, device cases etc.***
4. Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.

This consent form must be signed and returned prior to students being granted access to the internet and school devices/ resources.

Parents/Legal Guardians are encouraged to review and discuss with the student and answer any questions that they may have. Any queries in relation to this material should be directed to **your child's classroom teacher first.**

By signing this Consent Form, both Parents/Guardians and students are agreeing to the terms of access and acknowledge they will be responsible in the event of any breach and that appropriate disciplinary steps may result.

Parent/Guardian Consent

As the parent or legal guardian of the student named, I grant permission for them to access the provided technology resources, including digital platforms such as email and the internet.

I understand that access is granted to students subject to the restrictions contained and that if breached, consequences may follow.

I acknowledge that some material available on the internet may be objectionable. In addition to the Acceptable Use of Devices and Digital Resources consent, I understand it is my responsibility to implement appropriate restrictions for the student when accessing or sharing information or material over the internet.
BCE content filtering **only** applies when the device is connected to the BCE Wi-Fi network while on school grounds.

I understand that BCE devices may connect to home or other external internet services outside school hours, and these services do not include BCE internet filtering.

I accept responsibility for supervising the student's device use, internet access, and online behaviour outside of school, including ensuring safe and appropriate use when not on school grounds.

I understand that as outlined in the school and BCE responsibilities, devices may be remotely managed to ensure safe and secure use.

I understand that the school may disclose personal information about an individual to an external service provider for the limited purpose of storing and managing the information, for instance, when using public internet services to create learning and teaching content. The school may also disclose personal information to overseas service providers, for instance, when storing data with 'cloud' service providers, whose servers are situated outside Australia.

Whilst BCE takes all reasonable steps, in some cases, there may be an unauthorised disclosure of student personal information by third parties (for example, in case of a data breach of information held by the third party) which the school and/or BCE cannot control.

NAME: _____ **DATE:** _____

SIGNATURE: _____

Student Pledge

I agree with all requirements and all other relevant laws and restrictions in my access to the various technology resources through the Brisbane Catholic Education (BCE) network.

NAME: _____ **CLASS:** _____

SIGNATURE: _____ **DATE:** _____

Privacy collection statement

BCE and BCE Schools are committed to the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) (**Privacy Act**). BCE through its Privacy Statement and Information Collection Notice is collecting your information provided by you/the student on this form to insure the appropriate use of the BCE/school network and devices using the school network. The information will be used and disclosed by authorised BCE and BCE school employees for the purposes outlined on this form. Personal information collected on this form may also be used or disclosed to third parties where authorised or required by law. This information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your BCE School Principal or Brisbane Catholic Education Office directly at: *Phone: (07) 3033 7000 Address: 2A Burke Street, Woolloongabba Qld 4102 Australia*