



Student Device and Internet Resource Conditions of Use Statement

Computer and Internet resources have become critical to schools in facilitating and supporting learning and teaching. Technology resources are provided to students for educational purposes only. A breach of this statement will be managed under the School Behaviour Support Plan.

St Mary's Primary School has established significant computing and communication resources to support these activities. This includes technology provided on school grounds and school-owned IT devices. The school has specific requirements relating to the use of IT devices.

This document informs students of their responsibilities when using student devices, Internet and other information and technology resources, consistent with Brisbane Catholic Education (BCE)'s requirements, that all such resources are used in an ethical, legal and responsible manner.

These Conditions of Use are a concise summary of the more extensive terms contained within the Acceptable Use statement. By agreeing to abide by this Conditions of Use, you are also agreeing to abide by the Acceptable Use statement. It can be read in the BCE public website:

<https://www.bne.catholic.edu.au>

The requirements set out below apply to all school technology resources whether they are accessed through school or privately owned devices e.g. accessing school Internet services through a personal computer or mobile device.

Responsibilities of users

Permitted use of technology resources

1. Students must not:

- buy or sell items or services over the Internet
- access or enter chat rooms
- access, post or send inappropriate Internet or email content, especially content that is illegal, dangerous, obscene or offensive
- amend documents created by another student without that student's consent
- download, install or use unauthorised computer programs
- deliberately install computer viruses or other malicious programs
- gain unauthorised access to any system by any means
- use technology resources to attack or compromise another system or network
- access or intercept emails sent to other persons.

Confidentiality and cybersafety

2. Students should be aware that material they post on Internet sites (including social media sites) is public. The content of public posts may have personal implications for students. The content of posts also reflects on our school and school community. Once information is on the Internet it may not be possible to remove it.

3. Students must not display personal information about themselves or others in a way which is public. For example, students must not post their own or anyone else's address, telephone number or other personal details on the Internet or communicate these details in emails. Students must not distribute someone else's personal information without their permission.
4. Students should be aware that persons on the Internet might not be who they say they are and must not arrange to meet persons who they have met on the Internet.
5. Students should be aware that BCEO monitors use of devices.
6. Students should be aware that cloud-based tools and services may be used for data storage and learning opportunities. These services may store data on servers located outside Australia.

Cyberbullying and defamation

7. Students must not use email or the Internet to bully and/or harass others.

Security

8. Students must select a secure password and keep their username and password information private. The password must be changed regularly and should be difficult for other people to guess. Students must lock their device when not in use and log off at the end of sessions.
9. Students must not use another person's name and password to access resources.
10. Students must report a suspected breach of security to a teacher immediately.

Copyright

11. Students must note that material on the Internet is protected by copyright and must check the terms and conditions on websites before copying and/or downloading material.
12. Students must not use the school technology resources to copy, download, store or transmit any such material that may include music files, movies, videos or any other form of media.

Consequences following a breach of this statement

1. Loss or restriction of access to technology resources or formal disciplinary action for breach of school requirements.
2. Students and parents/legal guardians may be financially liable for damage caused to resources.
3. Cases of serious, deliberate, and/or criminal breach will be referred to the police and may result in civil or criminal proceedings.