TECHNOLOGY SUPPORT

Technology Use Policy

Background

Whitsunday Christian College provides students with computer and other technology facilities for educational use. The resources provided include computers, printers, interactive whiteboards, data projectors, access to email and the internet. Students may use these facilities for educational and research purposes only, including for class work, for the preparation of assignments and for the development in skills using a computer.

Obligations

Students should be aware of the following obligations in relation to their use of school technology:

1. Access and Security

Students will:

- not disable any settings for virus protection, spam and filtering that have been applied.
- ensure that communication through internet and online communication services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal account.
- log off at the end of each session to ensure that nobody else can use their account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
    - a message that was sent to them in confidence.
    - a computer virus or attachment that is capable of damaging recipients' computers.
    - chain letters and hoax emails.
    - spam, e.g. unsolicited advertising material.
- never send or publish:
    - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
    - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
    - sexually explicit or sexually suggestive material or correspondence.
    - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks
- ensure that services are not used for unauthorised commercial activities or any unlawful purpose.

- be aware that all use of internet and online communication services can be audited and traced to the internet accounts of specific users.

2. Privacy and Confidentiality

Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

3. Intellectual Property and Copyright

Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings.
- always acknowledge the creator or author of any material published.
- ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

4. Misuse and Breaches of Acceptable Usage

Students will be aware that:

- they are held responsible for their actions while using internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their account to access internet and online communication services.
- the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, Evaluation and Reporting Requirements

Students will report:

- any internet site accessed that is considered inappropriate.
- any suspected technical security breach

Offensive Material

The school administration has the final say in deciding what is or is not offensive in the school context, but will be guided by Section 85ZE of the Commonwealth Crimes Act which states that a person shall not knowingly or recklessly: 'Use telecommunication services supplied by a carrier in such a way as would be regarded by reasonable persons, as being in all circumstances, offensive.'

Use of the Internet in an offensive manner can result in criminal prosecution.

TECHNOLOGY SUPPORT

Compliance

Traditionally schools have opted to limit access to technology when a breach occurs. With technology now being a vital part of the classroom learning environment, we have decided to implement the following actions as a disincentive towards technology abuse.

Level 1 Breaches

Using the computer to download, watch, or stream videos not directly related to subject study requirements.
Using the computer to download, listen to, or stream music from the internet.
Playing computer games other than educational games as requested by the classroom teacher
Wasting time by looking up “funny pictures”, “fail blogs”, “cats”, playing with Sticky Notes etc.
Accessing and using social media.
Using classroom computers or technology without direct permission of teacher.

First Breach Detention same day or next if after break.	**Subsequent Breaches** Additional detentions. Possible internal suspension.

Level 2 Breaches

Using personal mobiles with internet tethering to avoid classroom monitoring, filtering and logging.
Using another student’s login details.

First Breach At least two detentions. Possible internal suspension.	**Subsequent Breaches** Internal suspension. Possible external suspension.

Level 3 Breaches

Accessing or creating pornographic, objectionable or offensive content.
Participating in cyber bullying.
Distributing copyright content via P2P or other file sharing mechanisms.
Intentionally or recklessly damaging computer hardware or devices.

First Breach Internal or external suspension of up to 5 days subject to review by Principal based on severity and level of involvement.	**Subsequent Breaches** Extended external suspension subject to review by Principal. Possible cancellation of enrolment.

Level 4 Breaches

Attempting to circumvent any security or access control.
Unauthorised modification of any system configuration.

Criminal offences under Queensland or Commonwealth legislation.

All Breaches
External suspension of minimum 3 days subject to review by Principal. Possible cancellation of enrolment. Queensland Police will be notified where required.