PIMPAMA
STATE SECONDARY COLLEGE

TOGETHER WE SUCCEED

P005
Student ICT Access and Usage

Policy & Information – Revision 24c

Effective from 30 September 2024

Last Updated September 2024

P + 61 7 5540 9333 **F** + 61 7 5540 7270 **E** admin@pimpamassc.eq.edu.au ABN 97 335 159 873
A Dixon Drive, Pimpama QLD 4209 Australia **PO** Box 201, Upper Coomera QLD 4209 Australia

This Page Intentionally Left Blank

P005
Student ICT Access and Usage
Policy & Information – Revision 24c

Contents

Document Changelog

Revision	Changes	User	Date
24a	2024 Policy Overhaul	Jack MACQUEEN	April 2024
24b	Updates to wording and content before publication	Elliot JACKSON	July 2024
24c	Add changes from feedback Finalise Formatting and Revision Numbering; Include Policy Number	Jack MACQUEEN Elliot JACKSON	September 2024

1.0 – Purpose of Student Access to ICT Equipment and Networks

To ensure young Queenslanders are well equipped to contribute fully to the 21st century economy and to enrich their learning experience through the access, creation and sharing of content. An essential tool for schools in the provision of innovative educational programs is the utilisation of intranet, internet, and network services. Therefore, access to these technologies is an increasingly essential part of the modern educational program provided in schools.

2.0 – What is Acceptable Use by a Student?

It is acceptable for students to use school computers, iPads, and network infrastructure for educational purposes such as:

- Completing assigned class work and assignments set by teachers.
- Developing literacy, communication, and information skills
- Creating text, artwork, audio, and visual material for publication on the Intranet or Internet, solely for educational purposes as supervised and approved by the school.
- Conducting research for school activities and projects
- Communicating with other students, teachers, parents, or experts in relation to schoolwork
- Accessing online references such as dictionaries, wikis, blogs, encyclopaedias, etc.
- Collaborating, researching, and learning through approved e-learning platforms including, but not limited to, Daymap, Stile, and QLearn.

3.0 – What is Unacceptable Use by a Student?

It is unacceptable for students to:

- Use mobile devices and wearable devices at school as outlined in the Away for the Day policy.
- Connect personal devices (e.g. phones, cameras, headphones, etc) to school equipment, networks, or power outlets without staff permission.
- Connect any devices (school or personal) to mobile hotspots or cellular connections while on school grounds or without explicit teacher permission on excursions.
- Bypass network filtering by any means including, but not limited to, proxy avoidance websites, virtual private networks (VPNs), or by use of mobile hotspots at school.
- Download, distribute, store, or publish offensive messages or pictures.
- Use school equipment and/or networks to harass, insult, or attack others.
- Deliberately waste printing, network bandwidth or other resources.
- Damage, deface, alter, or vandalize computers, printers, peripherals or network equipment.
- Install unapproved software onto workstations or shared devices.
- Violate copyright laws including plagiarism and piracy.
- Use school equipment and/or networks for communication not related to schoolwork or for access to social media.
- Disclose their login details to any other individual.
- Use another student or staff member's credentials to access networks, devices, services, or websites, including trespassing in another person's files, emails, etc.
- Enter a computer lab or use computers, iPads, or other equipment without staff permission.

4.0 – Consent

Some third-party services may require consent from parents/guardians before students can access them.

This can be due to certain services storing and/or publishing student personal information (such as name, date of birth, email address, etc.), student works, and image, video or audio recordings.

Any services requiring this information are reviewed by IT Services and the Department of Education before being used, however it is understood that some parents/guardians may not be comfortable allowing third parties to have access to their child's information.

As a result, consent must be obtained from parents/guardians before students may access these services.

In cases where a student has not yet obtained consent or parents/guardians have denied consent, that student is not to sign up for, sign in to, or disclose personal information to such a service.

5.0 – Monitoring

Use of the Department of Education's network (the network) (including internet and email) is logged, may be monitored, and where potentially unlawful conduct is detected, referred to law enforcement agencies.

Teachers may have the ability to monitor student's personal devices while in their classrooms.

IT Services has the ability to monitor all College owned devices both at school while on the network, and offsite though installed logging applications.

6.0 – Data Responsibility

Pimpama State Secondary College and the Department of Education take no responsibility for any data loss. Students should regularly back up their data.

Students have access to 100GB of cloud storage in OneDrive and 20GB of local network storage in H drive. Both should only be used for data relevant to schoolwork. Student H drives may be purged if an excessive amount of space is being taken up by content unrelated to schoolwork.

Data should not be stored locally on workstations or shared iPads. Not only is local data accessible to everyone else who uses a shared machine, it will also be erased during device updates.

7.0 – What Awareness is Expected of Students and Families?

Students and their parents should understand the responsibility and behaviour requirements that come with accessing the school's ICT network facilities and ensure they have the skills to report and discontinue access to harmful information if presented via the internet or e-mail.

Students should be aware that the misuse of school ICT resources will be managed within the guidelines of the Student Code of Conduct.

Consequences may include:

- Detentions
- Restricted, suspended, or withdrawn access to network/equipment for a period deemed appropriate.
- Removal from subjects that centre around the use of specialised ICT resources.
- Suspension from school for a period deemed appropriate.
- Referral to the Queensland Police Service
- Exclusion from school

The Internet provides access to information from a wide variety of organisations, subjects, people, and places with origins from around the world.

Access to the internet through the Department of Education network provides significant security in minimising the exposure of students to inappropriate, offensive and/or potentially harmful information.

Teachers will always exercise their duty of care, but protection, mitigation and discontinued access to harmful information requires responsible use by the student.

Some content and information which could be illegal, dangerous, or offensive may be accessed or accidentally displayed with or without the student's immediate knowledge.

Students are required to report any websites they may have inadvertently accessed that contain such material.

8.0 – ICT Network Access and Usage Agreement

This agreement (see separate page) must be signed by the student and by their parent or guardian on enrolment.

The guidelines will be discussed regularly with students in class and on assembly.

Any student who has not handed in a completed the signed ICT Network Access and Usage Agreement will be unable to access the network, including internet and email services until this is done.

This policy may be updated at any time without warning or notice. An up-to-date copy is available on the college website.

9.0 – Principal's Authorisation

Name	Megan Roderick
Date	05/09/2024
Signature