

## Use of Information and Communication Technologies (ICT)

At Pimpama State School, students are prepared for their future by accessing contemporary technologies and online platforms for learning. The Information and Communication Technologies (ICT) Acceptable Use Agreement outlines expectations for students.

This policy applies to Information Communication Technologies provided to students by the school, and Bring Your Own (BYO) devices brought to school to engage in our BYO Device programmes.

At Pimpama State School, students are expected to:

- use Information and Communication Technologies for learning purposes only. This may include:
  - engaging in assigned class work or assignments set by the teachers
  - accessing educational platforms or applications under the guidance of school staff
  - developing appropriate literacy, communication and information skills
  - authoring text, artwork, audio and visual material for publication on the intranet or internet for education purposes as supervised and approved by the school
  - conducting general research for school activities
  - communicating or collaborating with other students, teachers or experts in relation to school work
- treat ICT resources with respect and care
- login to online applications using the login details provided by the school
- be courteous, considerate and respectful of others when using ICT
- apply all school learning expectations to online environments (i.e. all of the school rules apply when using ICT)
- respect the rights of staff to teach using ICT
- respect the rights of students to learn using ICT

It is unacceptable for students to:

- use ICT in an unlawful manner
- download, distribute or publish menacing, intimate, harassing or offensive messages or online content
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use content, language and/or threats of violence that may amount to bullying and/or harassment, self-harm or stalking
- insult, impersonate, harass or attack others or use obscene or abusive language
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions for the use of social media, online email and internet chat
- use communication platforms (e.g. messenger, email) during school hours for purposes other than schoolwork

- send chain letters or spam email (junk mail)
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-device cameras anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- use the devices (including those with Bluetooth functionality) to cheat during exams or assessments
- use devices at exams or during class assessments unless expressly permitted by school staff

#### Misuse and breaches of acceptable usage:

- Information and Communication Technologies misuse will be dealt with in accordance with the *Disciplinary Consequences* section of the Student Code of Conduct.
- Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.
- The school reserves the right to restrict/remove access to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of ICT may result in the withdrawal of access to school supplied services.

#### Privacy and confidentiality:

- Students must not use another student or staff member's username or password to access the school network.
- Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program.
- It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

#### Intellectual property and copyright:

- Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.
- Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

#### Monitoring and reporting

- Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

- All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.