



St Joseph's School, Northam

ICT POLICY STUDENT ACCEPTABLE USE POLICY

The School's computing facilities are primarily intended for use in the teaching, research and administrative functions of the School. All students, teachers and parents must read and sign the Acceptable Use Policy.

Internet Usage

World Wide Web access, restricted by the School's filtering software, is the only service offered to students. Streaming of music, movies and whole episodes of programs is not an acceptable practice by students, unless directly linked to the class objectives and permission has been obtained from the class teacher, after authenticating classification level and relevant copyright restrictions. Staff and students are encouraged to check and respond to electronic mail (email) within a 24 hour period, in addition to other forms of communication where notices are posted.

The School's Internet service exists to provide access to curriculum related information as an educational resource.

Accessing inappropriate material is not permitted. Inappropriate material includes: pornography, extreme violence, gambling, terrorism, racism, political extremist, illicit drug manufacturing, advice or soliciting in these areas and 'Hacking' secure sites or material deemed inappropriate by staff of the School as directed by the School Principal.

Users will not record or process information, which might knowingly infringe any patent or copyright. Where another person's work is used it must be acknowledged accordingly, staff are required to direct students to the current referencing style guide as found in the school diary. Staff will inform students to review information published on the Internet for accuracy and reliability or may misrepresent a person or situation and use all sources wisely.

Under the Commonwealth Crimes Act, Division 474 Subdivision C (Offences related to telecommunications) of the Criminal Code (replacing Section 85ZE of the Commonwealth Crimes Act), states that a person shall not knowingly or recklessly use a telecommunication service supplied by a carrier to menace or harasses another person, or, use a telecommunications service supplied by a carrier in such a way as would be regarded by reasonable persons as being, in all circumstances, offensive.

In compliance of the Act, St Joseph's School students are:

- Permitted to download topic specific software on the School's computing facilities, after being acknowledged by the ICT Manager.
- Permitted to download appropriate text and graphic files to the School's computers and print these if related to School Curriculum.
- Able to access only computers designated by the seating plan provided by the teacher for that particular class.

Computing Facilities

With the CEWA Digital Transformation a range of online education tools are also encouraged to enhance the teaching and learning process, this will be primarily through (but not limited to) Office 365 and its applications and cloud-based storage.

Students in senior secondary will also through CEWA ViSN and outside providers be able to access online learning opportunities to complement our own course offering. The arrangements for this must be discussed with the School administration as there will be additional procedures to follow along with ongoing monitoring. The expectations for students involved with online courses in terms of ICT use, access to the Internet and social media, will still comply with these guidelines in addition to what policies are identified from the outside providers.

The School may consider punitive action against any person using the computing facilities if, after appropriate investigation that person is found to be:

- responsible for wilful physical damage to any of the computing facilities;
- in possession of confidential information obtained improperly;
- responsible for wilful destruction of information;
- responsible for deliberate interruption of normal services provided by the School;
- responsible for the infringement of any patent or the breach of any copyright;
- responsible for deliberate wastage of computer or system resources;
- gaining unauthorised access to accounts and passwords;
- gaining access to restricted sites or areas without appropriate authority.

Virus Control

Students are not permitted to use any removable media, such as USB drives and portable hard drives, with School equipment, unless it has been cleared by the ICT Manager. Staff and students will be encouraged to utilise the cloud storage as being developed by CEWA Ltd under the Leading Lights Digital Transformation project.

iPad Code of Conduct

The iPad is a tool to enhance student learning. Students are to abide by the School regulations concerning the acceptable use of electronic devices and any breach of this Code of Conduct will result in the loss of use of that device.

The use of iPads at St Joseph's School is a privilege, specifically designed to be a resource to enhance student learning and it abides by the School's ICT Policy for Computers. iPads are an expected integrated part of learning in Years 7-12 across all courses and encouraged for class use through personal devices in Years 5 and 6 and with class sets in all other years within our Primary school. Students in Years 10, 11 and 12 are permitted to bring personal laptops for class use. The appropriate use, internet usage, virus control and accessing online materials applies to these devices in the same manner as with the use of an iPad at school.

The following is to ensure that students are aware of their responsibilities when using any Mobile Devices at School. The use of mobile devices is dependent upon the student agreeing to the following statements:

Digital Etiquette

The standards of conduct expected by digital technology users

The following is a list of the expectations students are to understand and accept when using mobile devices at school. Students are expected to:

- Provide their device to teachers upon request.
- Follow all teacher directions including when to use the device.
- Have the volume of devices muted or use headphones as instructed by the teacher.
- Use appropriate manners when communicating electronically.
- Provide their device to parents/guardians upon request.
- School programs will take priority over personal data. Teachers have the right to delete personal data and download appropriate apps.
- A device can be confiscated by the teacher at any time if they are used inappropriately. Once confiscated, the device will be taken to Administration, recorded and stored for any time deemed appropriate by the teacher. (All incidences and parent communication will be logged into SEQTA or equivalent school-based behavioural monitoring tool).
- First confiscation – the device is taken to the Office and returned at the end of the day
- Second confiscation – the device is taken to the Office and returned at the end of the week
- Subsequent confiscations – will result in a meeting between the student, parent/guardian and the Head of School.

Digital Access & Use

For full participation as a 21st citizen and to engage with and benefit from a global community, students must be willing and able to adapt and adopt digital technologies to create solutions for everyday situations, enabling a fulfilling, engaging and productive participation in society.

- Students are expected to utilise access to various communications offered by the School in an appropriate and safe manner.

- Students are required to maintain their personal device by having it fully charged each morning, updated with the most recent operating system and cleaned, students are also encouraged to place their device into an appropriate cover for device safety.
- Students are required to report any damage immediately to Administration and complete an incident report if caused through malicious intent.
- Students are required to inform their teacher or others when using the camera and audio recording functions and are reminded that they must not publish photographs/video to any online network or shared space, unless instructed by a teacher.
- Students may not access their personal digital devices during recess or lunch.
- Students are required to have the device fully charged at the start of the day, and to keep chargers and cables in their secured lockers.
- Students are required to actively check their school email for communications, this is encouraged at least once every 24 hours.
- Students may not loan their device to another student and are responsible for the safety and use of their device.
- Students must only download appropriately rated applications, programs and audio-visual materials as outlined by the regulations from the Australian Federal Police.

Loss or Damage

It is the student's responsibility to make sure their personal electronic device (iPad or laptop for Years 10 to 12) is kept safe and secured when not in use. The student's parent/guardian will be required to cover the cost of repairing/replacing their child's device due to loss or damage. In the event of theft or deliberate damage whilst at school, students should report the incident immediately to their teacher or to the Head of School.

Where theft occurs whilst not at school, parents should report the incident to the Police. The school does not provide insurance cover for personal mobile devices brought to school. It is a parent's responsibility to ensure your child's device is covered when away from home.

Printing

Students must seek permission from a Staff Member before printing.

Consequences of Violating this Policy

Students will be dealt with through the normal School Behaviour Management Policy. However, in addition, access to computing facilities may be restricted or denied for periods deemed appropriate according to the magnitude of the offence.