



IMMACULATE HEART COLLEGE

Through Mary to Jesus: "The Way, the Truth and the Life"

John 14:6

ICT Acceptable Use Policy

Originally Released: October 2020

Date for Review: October 2024

Document # SM14



1. Introduction

Immaculate Heart College (IHC) is committed to providing its students and staff with the most effective Information Communication and Technology (ICT) hardware, infrastructure and online services in order to support and enhance teaching and learning within the College.

This Policy outlines the College's expectation of students and staff in utilising the College's ICT facilities in a responsible, efficient, ethical and legal manner, while conforming to the guidelines in this document.

2. Scope

Information and Communication Technology (ICT) means all computer hardware, software, systems and technology (including the Internet and email) and telecommunications devices in facilities that may be used or accessed from the College campus or connected to the College's communication network. This includes all personally owned devices whilst in use on the College campus or under supervision of College staff.

At IHC restrictions and policies are put in place to encourage the safe use of ICT within an educational context, to maximise educational outcomes and to ensure the safety of staff, students and community members.

3. Definitions

Information Communications Technology – the integration of computing, networking, and information processing technologies and their applications

Staff – all paid employees of IHC. The broader College community and the Board of Directors will be covered under the term 'staff'

3.1. Acronyms

ICT – Information Communications Technology

4. Responsibilities

The **Principal** is responsible for the implementation and routine review of this policy.



All staff, students and parents/carers are to acknowledge, encourage the safe use of, and ensure adherence to this policy.

5. Policy Principles

The College employs the following principles:

- a) ICT at Immaculate Heart College is provided for educational purposes only.
- b) The provision of ICT is a privilege which can be removed if College rules are broken.
- c) Staff and students using the College's ICT must not break state or federal laws (see supporting information).
- d) The College has the right to check all written, graphic, audio and other materials created, produced, communicated, stored or accessed on devices accessed by its staff and students, including emails.
- e) Students shall be made aware that access to ICT and in particular email and the Internet can expose them to inappropriate material or potential harm.
- f) Staff and students shall take personal responsibility when using the College's ICT services by protecting their personal information and data, maintaining the required level of security, respecting the privacy of others, respecting the legal boundaries of licensing and copyright, and using language appropriate to the College's expectations.
- g) Staff and students shall take personal responsibility when using the College's ICT devices by protecting and ensuring all equipment is treated with respect.
- h) Whilst staff and students are encouraged to explore and discover methods for utilising technology within the educational context, the College shall identify acceptable and unacceptable use of technology, email and internet systems and is committed to regularly updating this policy.
- i) If these conditions are breached, staff and students risk having disciplinary or legal action taken against them.



5.1. Acceptable and unacceptable use of ICT devices

Acceptable use of ICT devices includes:

- researching information relating to assessments, lesson content etc
- gathering specific information about subject/topics,
- emailing or electronically communicating with a teacher, student or member of the community for assistance with College related work

Staff and students shall at all times exercise caution as to the quality and accuracy of the information they are accessing or transmitting as they bear the responsibility for the content.

Unacceptable use of ICT devices includes:

- the transmission of any material in violation of any local, state, or federal laws
- being party to or participating in hacking, spamming, phishing scams, denial of service attacks and acts of fraud
- copying, downloading and/or sharing of commercial software or other media (eg music, videos or apps) in violation of federal copyright laws
- acts of plagiarism and/or breaching copyright laws, including software copyright and re-engineering software
- the use of profanities, obscene or other language that may be offensive to another member of staff, a student or member of the community, when using email and public forums such as social networks (eg Facebook and Twitter)
- being party to, participating in or failing to report acts of harassment, abuse, bullying, threats or acts which may be considered harmful either physically or emotionally to others
- committing any form of physical or digital vandalism
- use for commercial trade, conducting private business matters or use for personal gain
- use for all forms of gambling
- accessing, transmitting or distributing pornographic or obscene content, networks or websites
- knowingly creating and/or introducing electronic viruses or malware that can affect any system or network
- accessing another staff or student account or device without their consent



- taking, transmitting or distributing still or recorded images of any staff member or student without their documented consent
- bypassing the network security and filtering at the College via portable wireless devices (including smartphones), proxies or tunnelling
- removing the College network connection software, policies, certificates or antivirus software tools from any College provided devices
- participation in any intentional/malicious damage towards ICT devices
- committing any form of physical or digital vandalism to any College-owned device or its protective cover (including drawing, marking, scratching or ripping)
- a student using the device contrary to staff instructions during College hours (8:45am – 3:10pm). This includes accessing YouTube, social networks, and playing games.
- a student using the device contrary to parent or carer instructions after College hours. This includes accessing YouTube, social networks, instant messaging clients and playing games.

5.2. Digital access and device usage

Staff and students are expected to utilise access to various communications offered by the College in an appropriate and safe manner:

- Staff and students are required to inform others (the subjects) when using the camera and audio recording functions and are reminded that they must not publish photographs to an online network.
- Students may not play games on their device during College hours unless otherwise directed by a teacher.
- Students are required to have the device fully charged and present at school at the beginning of every school day.
- Staff and students are required to actively check their school email for College communication.
- Students may not use another student's device unless necessary for a class activity or they have permission to do so from its owner.
- Staff and students must only download appropriately rated application, videos and music to a College-owned device.



5.3. Loss or damage of College-owned devices

- In the event of loss or accidental damage, staff and students must report the incident to their teacher or the ICT Coordinator immediately.
- In the event of theft or deliberate damage while at College, staff and students must report the incident to their teacher or the ICT Coordinator immediately.
- Parent/carer of the student will be required to cover the cost of repairing/replacing the device due to loss or damage.

5.4. Student mobile phones and other electronic devices

The following 'common sense' rules are in place to educate students in the use of and management of their phone and other devices.

- If mobile phones and other electronic devices are brought to and kept at College, their use is entirely at their owner's risk. The College cannot accept any responsibility for theft, loss, or damage.
- Mobile phones should be kept in lockers (for senior students) or collected in PCG (for junior secondary and primary students) and NOT on their person between 8.45am and 3.10pm
- During the College day no ear buds should be seen outside of rooms where teachers are allowing them to be worn. At the discretion of individual teachers, as part of the learning environment, playing of music and videos may be appropriate
- All students should note that if a teacher asks for the student's phone during the College day, due to its improper use, it is important to respectfully hand the phone or device to the staff member. The student will be informed of collection protocol.

While mobile phones and smartwatches play a valuable role in our ability to communicate widely, they can cause issues when brought to the College.

- They can detract from the student's ability to engage in their work and in the day-to-day College life.
- Unfortunately, there is an increasing social trend that sees mobile phones and smartwatches used inappropriately as tools to bully, intimidate or harass.
- They are valuable items that can easily be lost, stolen or damaged.

The College acknowledges that parents may wish their child to carry a mobile phone/smartwatch for personal safety reasons however, the right of a student to have access to these devices must be balanced with the responsibility to use them safely and appropriately.



It is College policy that:

- Mobile phones/smartwatches must only be used by students before or after school.
- In class time, students may only use their mobile phones for educational purposes (eg to copy notes, take a picture in Art etc) with the express permission of the class teacher.
- Students should never photograph or record sound or capture other information during the school day without the express permission of the class teacher.
- Reports of all incidents of misuse of mobile phones/smartwatches will be recorded and placed in the student's file.
- Students are not permitted to use mobile phones/smartwatches during field trips, excursions or other off-campus supervised activities unless given permission to do so by relevant staff. Emergency communication arrangements with parents will be articulated in planning documents.

5.5. Monitoring of ICT services and devices for students

- All student mail and messaging can be monitored for inappropriate content and language and is reported upon accordingly.
- Student devices will be confiscated should they disrupt the learning of other students, be used inappropriately or if students take photos or videos of staff members or other students without their explicit consent.
- Student devices may also be confiscated and searched should the device contain inappropriate content or be involved in an incident of inappropriate behaviour.
- Personal restrictions and passcodes are to be placed on devices to protect personal data and unwanted use.
- In the event of any misconduct on the part of the student, a member of the senior staff may require access to personal restrictions passwords, passcodes and encryption.

5.6. Email

Staff and students are provided with their own email address for use at College. Staff and students found to have been using these resources inappropriately can expect disciplinary action.

Staff and students should be aware of the following expectations when using this system:

- Staff and students are expected to be sensible in their use of email. This includes NOT contributing to 'junk' or spam email.
- Staff and students will not publicly criticise, anger or abuse others.



- Students should never reveal personal details such as your name or phone number to others via email or via the Internet

It is unlawful to send electronic messages, such as emails, which:

- defame someone or an organisation
- infringe copyright laws i.e. reproduce or adapt copyrighted material by downloading and further disseminating the material
- contain statements which could constitute sexual discrimination or sexual harassment
- display sexually offensive or explicit material
- contain offensive or insulting statements based on race, colour or nationality of a person, and
- undertake activities that breach state and federal laws.

5.7. Internet usage

Staff and students should be aware of the following expectations:

- Staff and students are required to use the Internet responsibly. A rule of thumb for this is: "Would I be happy for the Principal to know what I was looking up?"
- Staff and students should not use the Internet to damage another persons' reputation.
- Students are NOT permitted to use proxy sites to circumvent the filtering software, and
- All access to the Internet can be monitored – it should be used it as an educative resource rather than a social/gaming network.

5.8. Legal implications

Staff and students are advised that the inappropriate use of electronic information can be a violation of local, state and federal laws. Please make yourself aware of the attached statutes that are applicable to your use of the Colleges ICT facilities.

6. Supporting Information

6.1. Copyright Act 1968 (C'wealth)

Staff and students may copy or otherwise deal with copyright material for the purpose of study or education. However, generally only the author of original material has the right to reproduce, copy, publish, perform, communicate to the public and make an adaptation of the copyright material.



Reference: <http://www.comlaw.gov.au/Details/C2012C00835>

6.2. Censorship Act 1996 (WA)

Staff and students must not use a computer service to transmit, obtain or request an article knowing that it contains objectionable and restricted material. It is an offence to possess or copy indecent or obscene articles or child pornography. Staff and students should be aware for their own protections that people who deal with such material commit an offence.

Reference: https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_s50012.html

6.3. Criminal Code (WA)

Staff and students should be aware that it is illegal to show offensive material to children under 16, and that if someone does show them offensive material that person is committing an offence. Racist harassment and incitement to racial hatred are also criminal offences.

Reference: https://www.legislation.wa.gov.au/legislation/statutes.nsf/main_mrtitle_218_homepage.html

6.4. Cybercrime Act 2001 (C'wealth)

Unauthorised access to or modification of data held in a computer and unauthorised impairment of electronic communication eg 'hacking' or infecting computer systems with a virus, are illegal

Reference: <http://www.comlaw.gov.au/Series/C2004A00937>

6.5. Privacy Act 1988 (Cth)

Staff and students should respect that the personal information of others is private. This Act covers the collection, use and disclosure, quality and security of personal information.

Reference: <http://www.comlaw.gov.au/Series/C2004A03712>

6.6. Other supporting documents

School Curriculum and Standards Authority Act 1997 (WA)

School Education Act, 1999 (WA)

School Education Regulations, 2000



7. Related Documents

The Emergency and Critical Incidents Policy is to be read in conjunction with the following College policies, or procedures, all of which can be found on the College Administration drive:

Type	Document	Doc #
Policy	Student Assessment and Reporting: Years 7-12	SM09

8. Review

This policy will be reviewed on a three yearly basis or as required continual improvement.

Year of Review	Authored by:	Reviewed by:	Reason for amendments or review
October 2021	S. Shaw	M. Gough	This is the first ICT Policy