



CATHOLIC EDUCATION
COMMISSION OF WESTERN AUSTRALIA

Policy:	Information and Communication Technology Use by Staff
Sub-Committee:	Audit and Risk Sub-Committee
Originally Released:	2001
Date for Review:	2016

1. Rationale

Information and Communication Technology (ICT) is utilised in schools for the purposes of learning, teaching and administration. ICT offers schools teaching and administrative tools that help students develop to their full potential and implement effective and efficient business practices. ICT also presents risks that must be understood and managed.

In accordance with the teachings of the Catholic Church, the practice of communication regardless of the medium, must be honest and reflect the highest standard of accountability and sensitivity to human rights and relationships.

As a privilege and gift from God, new learning needs to be accompanied by the development of a matching sense of social responsibility (Mandate, 72)

2. Definitions

Information and Communication Technology (ICT) means all computer hardware, software, systems, data, digital communications and technology including the internet, email and social media.

Defamation is a written or verbal statement that tends to lower another person's reputation in the eyes of ordinary members of the community, or leads people to ridicule, avoid or despise the person, or injures the person's reputation in business, trade or profession. There are a number of defences available against a claim of defamation including that the statement is true, or an honest opinion on a matter of public interest.

Harassment, Discrimination and Bullying means unlawful behaviour as defined in the CECWA Harassment, Unlawful Discrimination, Victimisation and Bullying policy.

Social media refers to internet based applications that allow users to share information and create communities (e.g. Facebook, Twitter).

Catholic School refers to an educational venue as defined in the Teacher Registration Act 2012 that is a part of the Catholic Education system in Western Australia. This includes schools as well as Early Learning and Care Centres.

3. Scope

This policy applies to all Catholic schools in Western Australia.

4. Principles

- 4.1 Schools have a responsibility to ensure appropriate precautions are taken to minimise the risk of exposure of inappropriate and offensive material to students and staff and ensure the dignity of the person is maintained and respected.
- 4.2 The use of ICT by staff, must comply with:
- child protection policies
 - relevant State and Commonwealth laws (a summary of these laws are outlined in the related documents section of this policy statement)
 - school rules or policies
- 4.3 Access to ICT is provided to staff to support their duties as staff members of the school.
- 4.4 All written, graphic, audio, video and other materials created, produced, communicated and stored using ICT for school purposes, are the property of the school and, as such, are subject to monitoring by the school. The school has the right to monitor all ICT logs which are the property of the school.
- 4.5 The use of ICT by staff, must not constitute unacceptable or unlawful behaviour (as outlined in procedures 5.2.2 and 5.2.3 of this policy).

5. Procedures

- 5.1 Schools shall develop, implement and enforce a policy on ICT use by staff.
- 5.2 The policy shall identify acceptable, unacceptable and unlawful use of ICT by school staff.
- 5.2.1 Acceptable use shall include but is not limited to:
- facilitating, gathering, creating and disseminating appropriate information for educational or related purposes
 - encouraging collaborative projects and resource sharing
 - supporting the transfer of data
 - fostering innovation
 - building broader infrastructure in support of education and research
 - fostering professional learning
 - undertaking school administrative functions
 - any other tasks that are for educational or related purposes or that support and promote the school and its ideals.
- 5.2.2 Unacceptable use shall include but is not limited to:
- accessing ICT systems without proper authorisation
 - transmitting or deliberately accessing, creating and/or receiving material that is inappropriate or offensive. Inappropriate or offensive material includes but is not limited to threatening, sexually explicit, offensive, defamatory or discriminatory materials, or material that may be harmful physically or emotionally. this may include bullying or harassment within and outside the school
 - unauthorised disclosure or communication of information concerning any password, identifying code or other confidential information without permission
 - interfering with or disrupting network users, services or equipment. Disruptions include but are not limited to unsolicited advertising, intentional propagation of viruses in any form or using the network to make unauthorised entry to any other machine or user file accessible via the school's network (i.e. 'hacking')
 - breaching copyright laws, including software copyright and reverse engineering of software or other laws governing intellectual property

- conducting private business for commercial gain or promotional material unrelated to a staff member's role in the school using the school's ICT
- bringing the school or Catholic Education into disrepute

5.2.3 Unlawful use shall include but is not limited to:

- defaming a person or an organisation using ICT
- infringing of copyright laws, i.e. reproduction and/or adaptation of copyrighted material by downloading and further disseminating the material
- use of ICT in a way that could constitute sexual discrimination or sexual harassment
- communicating with or contacting students on a personal level via written or electronic means without a valid context
- use of ICT that could constitute cyber bullying
- storing, displaying, creating or sending sexually offensive material
- use of ICT in a way that is discriminatory on the basis of, for example, race, sex, gender, disability or age
- undertaking activities which breach State or Commonwealth legislation

- 5.3 The policy shall contain a statement that personal use which does not constitute 'acceptable use' in accordance with the provisions of procedure 5.2 and is purely personal in nature shall be limited.
- 5.4 The policy shall state that unacceptable or unlawful use of ICT may constitute misconduct and/or serious misconduct and may result in termination of a staff member's employment contract.
- 5.5 The policy shall state that digital communications are subject to the records management processes of the school in accordance with the CECWA The Management of Confidential Information policy. From time to time, the school shall remind staff in writing either through the Staff Handbook or by email that emails sent by staff will be monitored. Schools shall also remind staff that any digital communication of an official nature, particularly to persons outside of the school, must be included in the school's records either in electronic or hardcopy form by the staff member.
- 5.6 The school's policy shall contain statements that appropriately identify and explain inappropriate or offensive material or conduct, such as material or conduct that:
- infringes a person's copyright or other intellectual property rights
 - is defamatory of a person or an organisation
 - contains sexually explicit, indecent or obscene or pornographic material
 - is discriminatory against a person on the basis of, for example, sex, race, religion, disability or age
 - deals with a person's personal information in a way that breaches privacy laws
 - constitutes racial harassment or incites racial hatred
 - constitutes harassment or bullying
 - is infected with a computer virus, would result in a breach of school security or disruption to the school's networks, or constitutes a 'cybercrime'
 - is otherwise contrary to school rules or policy
- 5.7 The use of ICT shall be informed by support documentation published on the CEOWA website.
- 5.8 Unlawful and/or serious misuse of ICT may result in the involvement of the Police and other Government Agencies.

6. References

Bishops of Western Australia 2009, *Mandate of the Catholic Education Commission of Western Australia: 2009-2015*

Catholic Education Commission of Western Australia policy statement 2-D8 The Management of Confidential Information

Catholic Education Commission of Western Australia policy statement 2-C4 Harassment, Unlawful Discrimination, Victimisation and Bullying (Staff)

7. Related Documents

Important statutes which are applicable to staff use of school ICT include:

Copyright Act 1968 (Cth)

Staff 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.

Equal Opportunity Act 1984 (WA)

This Act precludes:

- discrimination against persons on grounds of sex, marital status or pregnancy, family responsibility or family status, sexual orientation, race, religious or political conviction, impairment or age in education
- sexual harassment and racial harassment in the workplace and in educational institutions

This Act promotes:

- community recognition and acceptance of the equality of all persons regardless of their race, sexual orientation, religious or political convictions, impairments or ages

Censorship Act 1996 (WA)

Staff 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. Students should be aware for their own protection that people who deal with such material commit an offence.

Criminal Code (WA)

Staff 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.

Cybercrime Act 2001 (Cth)

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

Privacy Act 1988 (Cth)

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

CECWA Information and Communication Technology Use by Students policy

8. Related Proformas and other Forms

Proforma policy

9. Review History

Year of Review:	Reviewed by:	Amendments/Review
2001	SPC	Originally Released
2004	SPC	Reviewed
2006	SPC	Reviewed
2009	SPC	Reviewed
2010	CEOWA	Reformatted
2013	SPC	Reviewed
2017	CEWA Policy Group	Reformatted

10. Next Review

Year:	Sub-Committee Responsible
2016	Audit and Risk Sub-Committee