1. Rationale

Information and Communication Technology (ICT) has been introduced into schools allowing access to email and the internet and other telecommunication devices. The availability of such resources provides the opportunity for schools to help students develop their full potential. ICT provides significant educational value but can pose a risk of exposure to inappropriate and offensive material and personal safety.

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

2. Definitions

‘Information and Communication Technology (ICT)’ means all computer hardware, software, systems and technology including the internet, email and social networking (eg facebook) and telecommunication devices (eg mobile phones) in facilities that may be used or accessed from a school campus or connected to a school’s communication network.

Defamation is the publication, declaration or broadcast of material that is capable of lowering a Person’s reputation in the estimation of others.

Harassment, Discrimination and Bullying means unlawful behaviour as defined in the Catholic Education Commission Policy Statement 2-C4: ‘Harassment, Discrimination and Bullying’.

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 students to inappropriate and offensive material through the availability of ICT in schools.

4.2 The use of ICT, including the internet and email by staff, must not infringe:
• child protection policies
• relevant state and commonwealth laws (a summary of these laws are outlined in the Reference section of this policy statement)
• school rules or policy

4.3 Access to ICT and in particular email and the internet, is provided to staff to support their role as staff members of the school. Personal use should be limited.
4.4 All written, graphic, audio and other materials created, produced, communicated, stored or accessed on school ICT, including emails, are the property of the school, and as such, are subject to monitoring by the school.
4.5 The use of ICT, including the internet and email 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 and disseminating appropriate information for educational or related purposes
• encouraging collaborative projects and resource sharing
• assisting technology transfer
• fostering innovation
• building broader infrastructure in support of education and research
• fostering professional development
• undertaking 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 networks without proper authorisation
• transmitting or deliberately accessing 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 either physically or emotionally, including bullying or harassment within and outside the school
• unauthorised disclosing or communicating 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 and using the network to make unauthorised entry to any other machine accessible via the school’s network (ie ‘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
5.2.3 Unlawful use shall include but is not limited to:

- defaming of someone or an organisation in an email or webpage sent or produced using the school's ICT
- infringing of copyright laws, ie reproduction or adaptation of copyrighted material by downloading and further disseminating the material
- sending emails 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
- sending emails that could constitute cyber bullying
- displaying, storing or accessing sexually offensive material on the school’s ICT eg screensavers
- sending emails which are discriminatory on the basis of, for example, race, sex, gender, disability or age
- undertaking activities which breach state and 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 should 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 emails are subject to the records management processes of the school in accordance with the CECWA policy statement 2-D8: ‘The Management of Confidential Information’. 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 communication by email 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 use of the school’s ICT shall be informed by the guidelines in the CathEdNet Handbook as published from time to time.

6. References

Catholic Education Commission of Western Australia Policy 2-D8 The Management of Confidential Information
Catholic Education Commission of Western Australia Policy 2-C4 Harassment, Discrimination and Bullying

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.

8. Related Proformas and other Forms

Proforma available on System Communication Notice Board under M 'CECWA Policy statement proformas'

9. Review History

<table>
<thead>
<tr>
<th>Year of Review</th>
<th>Reviewed by</th>
<th>Amendments/Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>SPC</td>
<td>Originally Released</td>
</tr>
<tr>
<td>2004</td>
<td>SPC</td>
<td>Reviewed</td>
</tr>
<tr>
<td>2006</td>
<td>SPC</td>
<td>Reviewed</td>
</tr>
<tr>
<td>2009</td>
<td>SPC</td>
<td>Reviewed</td>
</tr>
<tr>
<td>2010</td>
<td>CEOWA</td>
<td>Reformatted</td>
</tr>
</tbody>
</table>