2.9 John Pujajangka-Piyirn Catholic School Information and Communication Technology use by Staff Policy

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.

DEFINITION

Information and Communication Technology (ICT) means all computer hardware, software, systems and technology (including the Internet and email) and telecommunication devices in facilities that may be used or accessed from a school campus or connected to a school's communication network.

PRINCIPLES

1. John Pujajangka-Piyirn Catholic School acknowledges that the availability of access to information on a global level poses a significant risk of exposure to inappropriate and offensive material.
2. John Pujajangka-Piyirn Catholic School accepts that the use of ICT, including the internet and email, must not infringe:
   - *Child protection policies;*
   - *Relevant state and federal laws (a summary of these laws are an attachment to this policy and form part of this policy);*
   - *School rules or policy; and, or unacceptable or unlawful behaviour (as outlined in procedure 2.2 and 2.3 of this policy).*
3. John Pujajangka-Piyirn Catholic School provides access to ICT and in particular email and the Internet to support the role of staff members. Personal use should be limited.
4. This policy works in conjunction with the John Pujajangka-Piyirn Catholic School Harassment policy.
5. John Pujajangka-Piyirn Catholic School accepts that the use of ICT, including the Internet and email, must not constitute unacceptable or unlawful behaviour (as outlined in Procedures 2.2 and 2.3 of this Policy).
6. Staff should be aware that 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.

PROCEDURES

1. John Pujajangka-Piyirn Catholic School is committed to ensuring that all staff are aware that unacceptable use of ICT (eg email and internet) within the school environment will not be tolerated under any circumstances and that disciplinary action will be taken against any staff member who breaches this policy.
2. John Pujajangka-Piyirn Catholic School shall identify acceptable and unacceptable use of ICT and is committed to regularly updating this policy.

2.1 Acceptable use may 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; and,
- Any other tasks that are for educational or related purposes or support and promote the school and its ideals.

2.2 Unacceptable use would include but is not limited to:

- Accessing networks without proper authorisation with mandatory reporting of any security flaws that are evident.
- 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, harassing materials, offensive, defamatory or discriminatory materials, or material that may be harmful either physically or emotionally, including bullying or harassment within and outside the school;
- Displaying culturally inappropriate or sensitive material without permission, which is accessible to students and public eg. Photographs of deceased persons.
- 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, and using the network to make unauthorised entry to any other machine 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; and,
- Conducting private business for commercial gain or promotional material unrelated to a staff member's role in the school using the school's ICT.

2.3 Unlawful use may include but is not limited to:

- Defamation of someone or an organisation in an email or webpage sent or produced using the school's ICT;
- Infringement of copyright laws, i.e. reproduction or adaptation of copyrighted material by downloading and further disseminating the material;
- Sending emails that could constitute sexual discrimination or sexual harassment;
- Displaying, storing or accessing sexually offensive material on the school's ICT e.g. screen savers;
- Sending emails which are discriminatory on the basis of race, sex, gender, disability or age; and,
- Undertake activities which breach state and federal legislation.
- Any software which is personally licensed or freeware may not be installed on a school computer without the Principal's permission.

3. Personal use which does not constitute 'acceptable use' in accordance with the provisions of procedure 2.1 and is purely personal in nature should be limited.
4. Unacceptable and/or unlawful use of ICT may constitute misconduct and/ or serious misconduct and may warrant disciplinary action. Any acts of continued misconduct may result in the termination of a staff member's contract of employment. Any act(s) of serious misconduct may result in the immediate termination of a staff member's contract of employment.
5. Emails are subject to the records management processes of the school.
6. All principles and procedures shall apply to guests and visitors to the school.
7. Visitors need to have permission from the principal to access the Internet on each occasion unless given a blanket permission.

Attachment: 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, and
- Promotes community recognition and acceptance of the equality of all persons regardless of their race, sexual orientation, religious or political convictions, impairments of age.

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 eg '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.

Year policy adapted :2004
Policy review: 2007