



# COMMUNICATIONS TECHNOLOGY POLICY

DATE: 4 DECEMBER 2007

---

## **Introduction**

The Pontifical Council for Social Communications (2002) has acknowledged the powerful contribution that the Internet<sup>1</sup> can make to the development of human life and culture. The world wide web, e-mail and other emerging technologies are transforming the worlds of work and commerce. The internet can foster prosperity and understanding among peoples and nations. The responsible use of freedom and democracy can be expanded by the emerging information and communication technologies. The internet is broadening educational and cultural horizons, breaking down divisions and promoting human development in a multitude of ways.

Whilst the potential for good in the internet has been acknowledged, so too has the potential for harm. Pope John Paul II (1999) has made the following observation in regard to the internet: “Yet, paradoxically, the very forces, which can lead to better communication, can also lead to increasing self-centredness and alienation.”

We find ourselves therefore in a time of both threat and promise. ... [We need to] rise to the challenge of new discoveries and technologies by bringing to them a moral vision rooted in our religious faith (John Paul II, 1999).

Catholic schools in South Australia are called to enter into a partnership with parents, in union with Christ's saving mission, to educate young people for active participation in the communities of Church and world (SACCS, 1991).

The responsible use of the internet has an important role to play in establishing characteristics like these in the Christian learning community. The use that educators make of the internet in their professional practice provides a very contemporary opportunity to witness to Christian values for students. Those who work in Catholic schools exercise a public ministry and, as such, are called to the highest professional standards of behaviour (see *Integrity in Ministry*, 1999).

This document sets out the security, administration and internal rules which should be observed when communicating electronically or using the Information Communication and Technology facilities provided by [*insert name of school*]). Users should be familiar with the terms of this Policy in order to minimise potential damage to your colleagues, students and the School, which may arise as a result of misuse of email or Internet facilities.

## **Policy Statement**

All workplace participants<sup>a</sup> of St Paul's College are to use the school's information and communications technology only in a way that enhances student and staff learning and contributes to the betterment and well-being of the community. The technology is to be used in harmony with the Catholic ethos of the school.

The school's information and communications technology includes the utilisation of any employer equipment, property or resource at any time, whether during working hours or not, and includes the use of remote access facilities.

**This Policy applies to all workplace participants of the School.**

---

## **The Policy in Practice**

**To give effect to this Policy the following understandings and procedures apply:**

### **1. A Workplace Facility**

- 1.1 The School's computer network is an educational and business facility provided by the school to be used primarily for educational or business purposes. Workplace participants, therefore, have a responsibility to use these resources in an appropriate, ethical, professional and lawful manner.
- 1.2 All email and Internet based message systems on the School's system will be treated as education or business related messages. Accordingly, one should not expect that any information or document transmitted or stored on the School's computer network is private.
- 1.3 Workplace participants are permitted to use the Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with participants' responsibilities and duties in the school, or with the School's functions.
- 1.4 However, any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.

### **2. Appropriate Use**

- 2.1 Individuals and/or the School may be liable for what is written or said in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.
- 2.2 The Internet or email should never be used for the following purposes:
  - (a) to abuse, vilify, defame, harass, degrade or discriminate (by virtue of sex, race, disability, religion, national origin or other);
  - (b) to send, receive or store obscene, offensive or pornographic material;
  - (c) to discuss or comment on the physical appearance of other persons (whether they receive the message or not);
  - (d) to harass any person whether through language, frequency or size of messages;
  - (e) to injure the reputation of the School and or the Church in a manner that may cause embarrassment to the employer or the Church;
  - (f) to offend the ethos and values of Catholic teachings;
  - (g) to spam, spoof or mass mail or to send or receive chain mail;
  - (h) to infringe the copyright or other intellectual property rights of another person;
  - (i) to perform any other unlawful or inappropriate act.

- 2.3 Workplace participants must not post messages to any Internet bulletin board, discussion group or any other accessible discussion forum unless the message is strictly work-related or has been authorised by the principal;
- 2.4 Excessive use of email or Internet facilities for personal reasons or inappropriate use may lead to disciplinary action including counseling, formal warnings and termination of employment or engagement. Any investigation would be carried out in accordance with the “Procedures for Dealing with Allegations of Misconduct”.
- 2.5 Any inappropriate material received by email should be deleted immediately and not forwarded to anyone else. It is particularly important to respond to inappropriate emails with an indication to the sender that such emails should not be sent in the future into, or within, the School's domain.
- 2.6 From time to time when accessing the World Wide Web users may be redirected to, or accidentally access, inappropriate material. These sites should be brought to the attention of the Principal or delegate in order for them to be blocked by the school's filtering software and to ensure that it is noted that the material was not accessed purposely.

### **3. Monitoring**

- 3.1 The contents and usage of email and Internet access may be subject to regular random monitoring by the School or by a third party on the School's behalf. This will include electronic communications which are sent or received, both internally or externally. Where inappropriate use is suspected through this means, or by other incidents, the Principal may authorise ICT personnel to examine the web access logs and or email accounts. No monitoring will occur without the Principal's permission except for normal logging of system usage to manage the network. Any investigation would be carried out in accordance with the “Procedures for Dealing with Allegations of Misconduct”.

### **4. Privacy**

- 4.1 In the course of carrying out duties on behalf of the School, staff may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another person except in accordance with the School's Privacy Policy or with proper authorisation.
- 4.2 The Privacy Act requires individuals and the School to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. When logged on, each person is responsible for the security of the computer and should not allow it to be used by an unauthorised party.
- 4.3 In order to comply with the School's obligations under the Privacy Act, the blind copy option should be used when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.
- 4.4 In addition to the above, users should be familiar with the National Privacy Principles ('NPPs') and ensure that the use of email does not breach the Privacy

Act or the NPPs. More information on the Privacy Act and how to comply with it, can be gained from the School Principal or the Privacy Officer.

- 4.5 Because of the risk of false attribution of email, a reasonable degree of caution should be maintained regarding the identity of the sender of incoming email. The identity of the sender should be verified by other means if there are reasons for concern.
- 4.6 Intentionally seeking information, obtaining copies or modifying files, tapes or passwords belonging to other persons, or representing others without express authority is prohibited.
- 4.7 Any deliberate attempt to subvert the security facilities may incur criminal or civil liability. Workplace participants are prohibited from infiltrating the system, damaging or altering software or data components of the system. Alteration to any system or network software or data component must only be undertaken if authorised by the Principal.

## **5. Distribution and Copyright**

- 5.1 When distributing information over the School's computer network or to third parties outside the School, users must ensure that they and the School have the right to do so, and that there is no violation of the intellectual property rights of any third party.
- 5.2 Software must not be copied without the express permission of the copyright owner. Copyright and other laws, together with licenses, protect most software. Workplace participants must respect and abide by the terms and conditions of software use and licenses.

## **6. Policy Updates**

- 6.1 This policy will be revised no later than September 2004.

## **7. Conclusion**

- 7.1 The terms of this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. Workplace participants are encouraged to act with caution and take into account the underlying principles intended by this Policy. Advice should be sought from the Principal where there is lack of clarity regarding appropriate action related to email or Internet use.

## **References**

- John Paul II. (1999). *World Communications Day*.  
National Committee for Professional Standards. (1999). *Integrity in Ministry*.  
Pontifical Council for Social Communications. (2002). *Ethics in Internet*.  
South Australian Commission for Catholic Schools [SACCS]. (1991). *Vision Statement*.

The following documents are useful resources and should be read in conjunction with this policy.

- Privacy Compliance Manual [www.ceo.adl.catholic.edu.au](http://www.ceo.adl.catholic.edu.au)
- Using the Internet Legally [www.ceo.adl.catholic.edu.au](http://www.ceo.adl.catholic.edu.au)
- Ethics in Internet [www.vatican.va](http://www.vatican.va)
- The Church and Internet [www.vatican.va](http://www.vatican.va)

This policy has been informed by documentation provided by Minter Ellison and the Industrial Relations Commission.

## **COMPUTER & NETWORK POLICY**

### **a) Guidelines**

- No user may use their account or another person's account to enter, copy, delete, modify, or tamper with system files, programs or another user's personal data.
- Users are not to use computers for anything other than schoolwork or related business work. *The use of web-based email/instant messaging, P2P software and online and offline non-educational games is **not permitted** and will result in immediate loss of access.*
- Users are forbidden to install or execute unauthorised software or media files.
- There shall be no violation of copyright laws.
- No user may tamper with the setup of the College's computers or intentionally introduce a virus. This also includes no downloading of programs, games or media files from the internet or modifying the appearance of the computer desktop in any way.
- No user may change the set up of hardware or the configuration of software in any way.
- No user may abuse hardware or software or use technology for any malicious purpose.
- Users may have to bear the full repair costs in the event of loss or damage caused through wilful damage to any computer system or peripheral device.
- Students are to use the internet only in relation to assignment research. Any other use of the internet is prohibited.
- The College has ownership of all equipment and may withdraw access to, and use of, the facilities at any time.
- Users must respect the rights of others to fair access and use of the facilities.
- School bags, food, drinks and chewing gum are strictly prohibited from the computer rooms.
- Students are not permitted to use or access the College computers or the network unless supervised by a teacher.
- All users should disclose any violations or potential loopholes in computer systems security to the Network Manager.

### **b) Email Policy**

#### **It is strictly prohibited to:**

- Send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify the Network Manager.
- Forward a message or copy a message or attachment belonging to another user without acquiring permission from the originator first.
- Send unsolicited email messages or chain mail.
- Forge or attempt to forge email messages, or disguise or attempt to disguise your identity when sending mail.

#### **Duty of care**

Users must take the same care in drafting an email as they would for any other communication. Confidential information should not be sent via email.

### **Personal usage**

Although the College's email system is meant for business and educational use, the College allows personal usage if it is reasonable and does not interfere with the normal routine of a working day.

### c) **Internet Policy**

If a user violates any of the acceptable use provisions outlined in this document, his / her account may be terminated and future access may be denied. Some violations may also constitute a criminal offence and may result in legal action. Any user violating these provisions, applicable State and Federal laws, is subject to loss of access privileges and any other College disciplinary options.

#### **Acceptable Use**

- Must be in support of education and research consistent with College policy.
- Must be consistent with the rules appropriate to any network being used / accessed.
- Unauthorised use of copyrighted material is prohibited.
- Publishing, downloading or transmitting threatening or obscene material is prohibited.
- Distribution of material protected by trade secret is prohibited.
- Use of commercial activities is not acceptable.
- Product advertisement or political lobbying is prohibited.

#### **Privileges**

- Access to the Internet is not a right, but a privilege.
- Unacceptable usage will result in cancellation of account, and possible disciplinary action.

#### **Etiquette**

- Be polite.
- Do not use vulgar or obscene language.
- Use caution when revealing your address or phone number (or those of others).
- Electronic mail is not guaranteed to be private.
- Do not intentionally disrupt the network or other users.
- Abide by generally accepted rules of network etiquette.
- If you identify a security problem, notify a system administrator immediately.
- Do not show or identify a security problem to others.
- Do not reveal your account password or allow another person to use your account.
- Do not use another individual's account.
- Attempts to log on as another user will result in cancellation of privileges.
- Any user identified as a security risk or having a history of problems with other computer systems may be denied access.
- User must notify the system administrator of any change in account information.
- User may be occasionally required to update registration, password and account information in order to continue Internet access.
- College has access to all user access requests, and will monitor websites as necessary to assure efficient performance and appropriate use.

#### **Vandalism / Harassment**

- Vandalism and / or harassment will result in the cancellation of the offending user's account.
- Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet or other networks. This includes, but is not limited to, creating and / or uploading computer viruses.
- Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes, but is not limited to, the sending of unwanted mail.

**Penalties**

- Any user violating these provisions, applicable State and Federal laws or posted College policy is subject to loss of network privileges and any other College disciplinary options, including criminal prosecution.
- All terms and conditions as stated in this document are applicable to all users of the network. This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet facilities and is not necessarily exhaustive.

By pressing on the OK button you are stating that you agree to the above policy when using the Internet.