Our Lady of Hope School
Greenwith

POLICY DOCUMENT

Communications Technology
Contents

Introduction 3
Policy Statement 4
The Policy in Practice 4
1. A Workplace Tool 4
2. Appropriate Use 4
3. Monitoring 5
4. Privacy 6
5. Distribution and Copyright 6
6. Policy Updates 7
7. References 7
8. Appendix A Professional Development Statement 8
Introduction

The Pontifical Council for Social Communications (2002) has acknowledged the powerful contribution that the Internet\(^1\) 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 Our Lady of Hope 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.

\(^1\) Accessing the internet may include but not limited to Web surfing, File Transfer Protocol (FTP), discussion and chat facilities, Telnet and email.
Policy Statement

All workplace participants and students of Our Lady of Hope 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 school equipment, property or resource at any time, whether during working/school hours or not, and includes the use of remote access facilities.

This Policy applies to all workplace participants and students of the School.

The Policy in Practice

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

1. **A Workplace/School 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 and students, 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 computers, 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 Students are permitted to use the computers, Internet and email in line with the "Student ICT Agreement" at Appendix B.

1.5 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 and students must not post messages to any Internet bulletin board, discussion group or any other accessible discussion forum unless the message is strictly work/school-related or has been authorised by the principal;

2.4 Excessive use of email or Internet facilities for personal reasons or inappropriate use by workplace participants 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 by workplace participants 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 workplace participants 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.

2.7 The appropriate use of computers, the Internet and email is defined in the "Student ICT Agreement" at Appendix B.

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. Where there is a workplace participant involved, 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 and students 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 and students 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 2016.

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 computer, email and Internet facilities. All users 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 computer, email or Internet use.

References


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

- Privacy Compliance Manual  www.ceo.catholic.edu.au
- Using the Internet Legally  www.ceo.catholic.edu.au
- Ethics in Internet  www.vatican.va
- The Church and Internet  www.vatican.va

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

Attachments:
Appendix A – Professional Development Statement
Appendix B – OLOH Student ICT Agreement

[Signatures and dates]

(Chairperson)  25/3/12  (Principal)  25/3/13
(Date)  (Date)

SBP Number 2  Page 7 of 7  Date: 2013
Review Date: 2016
PROFESSIONAL DEVELOPMENT STATEMENT

Planning for the provision of professional development for the successful integration of information technology into all areas of the curriculum at Our Lady of Hope School is regarded as a very high priority. The development strategies are aimed at ensuring that:

- Teachers and principals are skilled in using learning technologies to improve teaching and learning;
- Students and teachers routinely use technology as a tool for student learning and teacher professional development.

Essential elements of planning for effective professional development include:

- Naming of professional development as a management objective in the School's development Plan;
- Budgeting for such professional development;
- Identification of individual staff and whole staff professional development needs in the area of information technology;
- Planning for and provision of release time to attend professional development sessions;
- Provision of technical support for the computer network so that teachers' time will not be taken up with technical failures;
- Technical ability to use learning technologies for personal and professional purposes;
- Ability to effectively integrate and manage the use of learning technologies in classroom programs;
- Ability to evaluate the use and effectiveness of specific learning technologies;
- Ability to record and monitor student progress using information technology;
- Leadership support for the above.
Parents & Caregivers,
We ask you to work through this with your child, to ensure that they understand the school’s policy and expectations regarding the use of ICT, and what they are agreeing to.

Teachers will also go through this agreement with the children early in the term to ensure they understand the expectations. If you have any questions regarding this please discuss these with your child’s class teacher in the first instance.

**O.L.O.H STUDENT ICT AGREEMENT**

It is a privilege **not** a right to use the computers, internet and digital cameras, and it must be used in a responsible and sensible manner.

If you agree to the following conditions, please sign below and return to your class teacher.

You will **NOT** be able to use any of the above mentioned unless this agreement is signed and returned to school.

- ✓ I will seek permission from my class teacher before using the internet and email.
- ✓ I will only use the internet in the presence of my class teacher.
- ✓ I will not load any material on the school computers that are irrelevant to my learning. For example; music, movies, images etc
- ✓ I will only have school related data on the USB I use at school.
- ✓ I will only download material that is relevant to my learning.
- ✓ I am responsible for remembering my password and I must keep it secret.
- ✓ I will only use the internet to find information relevant to my school work.
- ✓ I will immediately close down any sites or information that are inappropriate and will report this immediately to my teacher and I will NOT revisit the site again.
- ✓ I will only use my first name and not give out surnames, addresses, telephone numbers on the internet.
- ✓ I will only send emails to addresses that my teacher has approved.
- ✓ I will use appropriate language at all times when using the computer.
- ✓ I will not use email to harass anyone.
- ✓ I will use all digital cameras and computers with care AT ALL TIMES.
- ✓ I will use digital cameras for educational use only, and seek permission of any person I need to photograph.
- ✓ I am aware that there will be consequences for misusing any ICT equipment and I am also aware that if I do NOT follow the above agreement it will lead to a loss of my privileges to use them for a period of time.
- ✓ I am aware that if I intentionally access internet sites of a sexual and/or violent manner this will lead to suspension and loss of the privilege of using the technology for one school month. Any further breaches could lead to expulsion from the school.
- ✓ I am also aware that my parents/caregivers will be notified by a letter if I do not follow this agreement.

<table>
<thead>
<tr>
<th>Student Name:</th>
<th>Year Level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Signature:</td>
<td>Class Teacher:</td>
</tr>
<tr>
<td>Parent/Guardian Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>