

Workplace Internet, Email and Network Usage

(Please retain for your records)

Rationale

“Information and Communications Technology in the workplace raises questions about the supervision of its use. This technology includes email and access to the Internet. The computers and internal network involved are controlled by the organisation and management has the responsibility for issuing clear instructions for their proper use. Without clear instructions, the proper use of email and web browsing may not be clear to many in the workplace.” Australian Privacy Commission 2005 (<http://www.privacy.gov.au/internet/email/>).

This policy statement is designed to assist in the development of good practice. Policy Guidelines for **Workplace Internet, Email and Network Usage** set out information for employees of the Catholic Education Office of Wilcannia-Forbes regarding the proper and permitted use of the network, including internet, email and web browsing. Central to this policy is the implementation of a Code of Practice for all diocesan schools and the Catholic Education Office.

Employees are urged to ensure that their professional and personal behaviour in relation to email and web use is consistent with this Policy. Unacceptable uses of the network and breaches of this Policy may require disciplinary procedures.

Definitions

For the purposes of this Policy, the following definitions apply:

Employees – people employed in teaching and non-teaching positions in schools and the Catholic Education Office, Diocese of Wilcannia-Forbes.

Employer – Anthony Morgan, Director of Schools on behalf of the Trustees of the Diocese of Wilcannia-Forbes.

NB It is the responsibility of employees to familiarise themselves with the contents of this Policy.

Implementation

1. The Catholic Education Office provides computers and Internet access to support the educational mission of the schools and the administration of the system of schools, and to enhance the curriculum and learning opportunities for student, school and administrative opportunities for Catholic Education Office staff.
2. Employees are to utilise Catholic Education Office's computers, networks and Internet services for office and school-related purposes and performance of job duties. Incidental personal use of Catholic Education Office computers is permitted, as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users. 'Incidental personal use' is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this Policy and all other related procedures and rules.
3. Employees are expected to use appropriate judgement and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.
4. To ensure that the Catholic Schools' networks and Internet connections function effectively and to make users aware of the responsibilities and expectations of using these resources a Code of Practice will be implemented in all diocesan schools and the Catholic Education Office.

Privacy Expectations and Intellectual Ownership

5. System administrators are able to access user data and log network use as part of their role. In reviewing and monitoring user accounts and information, the Catholic Education Office systems administrators will respect the privacy of individuals. These people must not divulge or disclose such information to others unless required by the Executive Officer, Administrator- I.T. or State or Commonwealth Law. (ref. National Privacy Principles 2001).

Privacy Expectations & Intellectual Ownership (Cont)

6. System administrators within the Catholic Education Office and schools include the Administrator- I.T. and nominated IT personnel.
7. Materials produced, sent and kept by employees, remain the property of the Catholic Education Office, Diocese of Wilcannia-Forbes.

Emails

8. The sender of an email has no control over the future distribution of the message.

The following are technical realities of the use of emails:

- Email should be regarded as insecure unless it has been encoded or encrypted.
- Most software used to operate networks including web servers, mail servers and gateways logs transactions and communications. These logs will normally include the email addresses of senders and recipients and time of transmission. System administrators are capable of reading the contents of emails sent and received by the Catholic Education Office network.)

Appropriate Use of Email in the Workplace

- 8.1 The use of email to communicate to others in the organisation on work-related matters, connected with the goals and purposes of the Catholic Education Office.

Unacceptable Use of Email in the Workplace

- 8.2 The use of email to:
 - Harass or discriminate against other employees either in emails.
 - Send abusive email.
 - Defame other employees, the Catholic Education Office, or another individual or organisation.
 - Disclose personal information or contact details about another employee.
 - Receive, maintain or transmit pornography either in emails or as screensavers.

Unacceptable Use of Email in the Workplace (Cont)

- Read another person's email without their expressed consent.
- Send on chain letters which may be interpreted as harassment by others.
- Send and forward to others, jokes which may amount to sexual harassment or discrimination via email on an intranet or the Internet.
- Send anonymous messages which contain no details of the sender's name and affiliation.
- Waste resources – time, or the capacity of the system or the equipment.
- Without authority, destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of computer-based information and/or information resources, including, but not limited to, uploading or creating computer viruses.
- Use a third party's copyright material.

Internet and Web Browsing

9. Most content made available on web sites (including text, images, software, sound and film clips) is protected copyright material. Accordingly, when browsing the world wide web, copyright laws must be respected. However, under the Copyright Act, the making of a temporary reproduction of a work in the course of browsing the Internet is not an infringement.

10. The issue of appropriate usage may be harder to define in respect to web browsing. It may not be possible to tell if a web page is relevant until it has been read. The operation of web search engines can result in surprising and irrelevant results. Links on web sites may also be misleading.

11. Schools and staff have a dual responsibility to protect students from offensive material, and to ensure that neither principals, staff nor students may be liable for transmitting offensive material.

Appropriate Use of the Internet in the Workplace

The use of the Internet to access information and resources for work-related matters, connected with the goals and purposes of the Diocese of Wilcannia-Forbes.

Unacceptable Use of the Internet in the Workplace

12. The use of the Internet to:

- Download sexually graphic material.
- Access web sites which are pornographic.
- Participate in 'Chat Groups' unrelated to work.
- Subscribe to listservs unrelated to work.
- Violate any State, Commonwealth or International Law.
- Conduct any business activity for financial gain or commercial purposes.
- Download information or software, eg games, for the purpose of providing to an unauthorised third party.
- Violate Catholic Education Office or third party copyright or licensing agreements or other contracts.
- Seek to gain unauthorised access to any resources within or outside of the Catholic Education Office.
- Waste resources – time, or the capacity of the system or the equipment.

Computer and Network Use

13 Note:

- Extensive use of the network for personal and private business is prohibited.
- Network accounts are to be used only by the authorised owner of the account for the authorised purpose.
- Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.
- All communications and information accessible via the network should be assumed to be private property.
- No use of the network shall serve to disrupt the use of the network by others.
- Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
- The installation of unlicensed software for use on school or office computers is prohibited.
- Staff choosing to authenticate a personal owned laptop on a school's network must sign an end user agreement that outlines the level and type of support available and the end users responsibility in managing the laptop.

Consequences of Inappropriate Behaviour

- 14 An employee's conduct and behaviour in relation to the use of email, internet and web browsing may be deemed inappropriate if the contents of this Policy are found to have been breached.

- 15 Failure to comply with this Policy governing computer use may result in disciplinary action, up to and including discharge.

I have read this policy carefully and agree to abide by the directions set out in the policy. In particular I have registered the directions in clauses 2, 3, 5, 7, 8.2, 12, 13, 14, and 15.

Should you have any matters which need clarification in relation to workplace internet, email and network usage, the following website may be helpful <http://www.oaic.gov.au/>