



Computer Facilities and External Networks – Acceptable Use

Related Policies

None

Purpose

This policy supports and describes the process for the acceptable use of Catholic Education Office computer facilities and external networks, including the internet, for the purposes of administration and the fostering of educational activities in Archdiocesan schools, the CEO and other CEO non-school workplaces.

Policy

- Access for all authorised users is for educational administration and/or learning and teaching purposes, and reasonable personal use.
- All CEO work places are responsible for establishing and maintaining on-site procedures for a secure computing environment with regard to authorised access, student supervision and acceptable use by staff and students consistent with the role and functions of the CEO, as well as the Copyright Act 1968 and Privacy Act 1988.
- Each CEO work place is expected to implement a Code of Practice for acceptable use (see attached example).
- The CEO, Archdiocesan schools and other non-school workplaces are required to implement the attached CEO Code of Practice.

Definitions

Computer Facilities and External Networks includes computers, local area networks, connections to external electronic networks, and subscriptions to external network services.

Licensed Software collectively refers to copyrighted and proprietary programs, data and documentation.

Internet refers to the global network of multi-platform smaller computer networks which allows the user to access information and communicate electronically.

Responsibilities

1. It is the responsibility of the CEO to:
 - 1.1 ensure that the authorised use of computer facilities and external networks, including the internet, relates to CEO business and is consistent with principles, regulations and laws relating to the privacy and safety of school students and CEO staff.

Computer Facilities and External Networks – Acceptable Use

2. It is the responsibility of all users to:
 - 2.1 obtain authorisation prior to using CEO computer facilities and external networks, including the internet, through the use of passwords and user identification.
3. It is the responsibility of Principals to:
 - 3.1 implement a School Code of Practice (use attached example as a guide to developing a school-based code);
 - 3.2 develop and implement a Student Code of Practice;
 - 3.3 ensure that Codes of Practice are available to and understood by all users;
 - 3.4 ensure that student access will be appropriately supervised as determined by the school;
 - 3.5 highlight to users the possible dangers of communicating personal information on the internet;
 - 3.6 obtain from the person with parental responsibility, annual written permission for students under 18 years of age to publish or transmit student work which may or may not include identifying student information. This includes any publishing of student work which may be done by a third party on their behalf;
 - 3.7 obtain written permission from students 18 years and over (refer to previous point); and
 - 3.8 monitor reasonable personal use by school staff.
4. It is the responsibility of CEO Heads of Division to:
 - 4.1 implement the CEO Code of Practice (attached);
 - 4.2 ensure that Codes of Practice are available to and understood by all users.
 - 4.3 monitor reasonable use by CEO Division Staff

Procedures

1. Acceptable uses are those:
 - 1.1 related to learning and teaching;
 - 1.2 related to educational administration.
2. Supervision of computer facilities and external networks.
Supervisors must take measures to ensure that computer networks are used in an acceptable manner.

Procedures to ensure this must include:

- 2.1 a school code of practice;
- 2.2 a CEO code of practice;
- 2.3 security procedures to ensure authorised access to computing network;
- 2.4 appropriate supervision of users;
- 2.5 the use of appropriate software, either on site or by the service provider, to allow access to appropriate online sites only; and
- 2.6 education programs that focus on ethical and acceptable uses of the internet, as well as correct online etiquette.

Computer Facilities and External Networks – Acceptable Use

3. Prohibited Activities.
 - 3.1 For students under 18 years of age, publishing or transmitting student work which may or may not include identifying student information, without annual written permission from the person with parental responsibility. Students 18 years and over must give their own written permission.
 - 3.2 Uses that unduly interfere with the work of other users of the network or with their host systems, or that seriously disrupt the network, or that result in the loss of a user's work.
 - 3.3 Transmitting or deliberately accessing material, the use of which may be harmful emotionally or physically (eg, instructions to make a bomb).
 - 3.4 Uses that contravene existing laws regarding transmitting or deliberately accessing information (eg, hacking), which contains profane language or panders to bigotry, sexism, or other forms of discrimination.
 - 3.5 Transmitting or deliberately accessing information which contains sexually explicit material.
 - 3.6 Uses that violate Commonwealth, State or Territory laws.
 - 3.7 Uses that violate the privacy of individuals.
 - 3.8 Communicating any information concerning any password, identifying code, personal identification code or other confidential information without the permission of its owner or the controlling authority of the computer facility to which it belongs.
 - 3.9 Creating, modifying, transmitting or using any computer program or instructions intended to gain unauthorised access to, or make unauthorised use of, a computer facility, software or licensed software.
 - 3.10 Use of the CEO's computing network for commercial or private purposes.
 - 3.11 Creating, modifying, transmitting or using any computer program or instructions intended to obscure the true identity of the sender of electronic mail.
 - 3.12 Accessing or intentionally destroying software or licensed software in a computer facility without the permission of the owner of such software or licensed software or the controlling authority of the facility.
 - 3.13 Making unauthorised copies of licensed software.
 - 3.14 Communicating any credit card number or other financial account number without the permission of its owner.
 - 3.15 Effecting or receiving unauthorised electronic transfer of funds.
 - 3.16 Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.
 - 3.17 Using the computer facilities and external networks in a manner inconsistent with the CEO's contractual obligations to suppliers of computer facilities and external networks or with any published CEO policy.

References

Acceptable use of (IT) Information technology Resources Statement is located at <http://www.decs.act.gov.au/policies/pdf/AcceptableAccessUseOfITresources.pdf>

Computer Facilities and External Networks – Acceptable Use

Forms

Archdiocese of Canberra and Goulburn Catholic Education Office - Code of Practice – Acceptable Use of Computer Facilities and External Networks.

Example of a School's Code of Practice - Acceptable Use of Computer Facilities and External Networks.

Approved by:	CEO Heads of Division
Issuing Group:	Information and Communications Technology Services Division
Implementation Date:	January 2005
Supersedes Policy Dated:	April 2001
Revision Date:	2008
CEO Contact Officer:	Head of the Information and Communications Technology Services Division

Archdiocese of Canberra and Goulburn Catholic Education Office Code of Practice

ACCEPTABLE USE OF COMPUTER FACILITIES AND EXTERNAL NETWORKS

Purpose

This code of practice has been developed for all CEO and other non-school workplace staff and is consistent with the CEO's policy on *Acceptable Use of Computer Facilities and External Networks*. Division Heads are responsible for ensuring that staff are familiar with the policy and Code of Practice, and operate within the parameters of these documents. This includes supervision of students who may be utilising facilities within the CEO's offices.

MANDATORY PROCEDURES

Security

- ensure your login and password are unique (i.e. don't use shared passwords)
- log your workstation off the network before leaving the building

It is Acceptable to:

- facilitate and disseminate knowledge; encourage collaborative projects and resource sharing; aid technology transfer; foster innovation; build broader infrastructure in support of education and research; foster professional development; undertake administrative functions and any other tasks which support the business of the CEO.

It is Unacceptable to:

- access networks without proper authorisation;
- undertake illegal activities as defined under the Australian Commonwealth Government Telecommunications Act 1989, or other applicable State and Commonwealth laws;
- transmit or deliberately access and/or receive material that may be considered inappropriate, including threatening, sexually explicit, or harassing materials, offensive or discriminatory material or material that may be harmful either physically or emotionally;
- communicate any information concerning any password, identifying code, personal identification code or other confidential information;
- interfere with or disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and using the network to make unauthorised entry to any other machine accessible via the network;
- breach copyright laws, including software copyright;
- use material downloaded from a network without correct referencing.

Employees of the Archdiocese of Canberra and Goulburn Catholic Education Office may access the Internet via the CEO Local and /or Wide Area Network after signing the following declaration.

I declare that I have read and understood the Archdiocese of Canberra and Goulburn CEO's policy on Acceptable Use of Computer Facilities and External Networks and the accompanying Code of Practice.

Surname: _____ Given Name: _____

Location: _____ Position: _____

Signature: _____ Date: ____/____/____

This original declaration is to be returned to:-

Office use only

Head
Information and Communications Technology Division
Archdiocese of Canberra and Goulburn
Catholic Education Office

Date: ____/____/____

Signed _____

Example of a School's Code of Practice
Acceptable Use of Computer Facilities and External Networks
[to be used by schools as a guide to developing a school-based Code of Practice]

Purpose

This Code of Practice has been developed for staff at _____ {name of school} and is consistent with the CEO's policy on *Acceptable Use of Computer Facilities and External Networks*. Principals are responsible for ensuring that staff have read the policy and Code of Practice, and operate within the parameters of these documents.

MANDATORY PROCEDURES**Security**

- passwords are only to be made known to authorised staff;
- passwords for administrative networks are only to be given to authorised staff;
- students may be given low level access only to educational networks;
- identifying student information can only be published on the internet with the written permission of the parent/carer.

Supervision

- student activity on computer networks will be supervised appropriately by staff. Staff will take all reasonable steps to ensure that student activity on networks is in accordance with the School Code of Practice.

It is Acceptable to:

- facilitate and disseminate knowledge; encourage collaborative projects and resource sharing; aid technology transfer; foster innovation; build broader infrastructure in support of education and research; foster professional development; and any other tasks which support the educational goals of the CEO.

It is Unacceptable to:

- access networks without proper authorisation;
- undertake illegal activities as defined under the Australian Commonwealth Government Telecommunications Act 1989, or other applicable State and Commonwealth laws;
- transmit or deliberately access and/or receive material that may be considered inappropriate, including threatening, sexually explicit, or harassing materials, offensive or discriminatory material or material that may be harmful either physically or emotionally;
- communicate any information concerning any password, identifying code, personal identification code or other confidential information;
- interfere with or disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and using the network to make unauthorised entry to any other machine accessible via the network;
- breach copyright laws, including software copyright;
- use material downloaded from a network without correct referencing.

Name of School: _____ Date Code implemented ____/____/____

Staff of _____ {name of school} may access the Internet after signing the following declaration.

I declare that I have read and understood the Archdiocese of Canberra and Goulburn Catholic Education Office's policy on Acceptable Use of Computer Facilities and External Networks and Code of Practice designed for _____ {name of school}.

Surname: _____

Given Name: _____

Location: _____ Position: _____

Signature: _____ Date: ____/____/____

This original declaration is to be returned to:

Principal: _____ Date: ____/____/____

Name of school: _____ Signed: _____

A COPY WILL BE RETURNED TO YOU FOR YOUR RECORDS