Catholic Education Office – Diocese of Wollongong

Policy on the Acceptable use of the Internet, Intranet, e-mail and other Electronic Communication Devices

This document sets out guidelines for employees of the CEO and school for acceptable use of electronic mail (e-mail), for employees access to the CEO and/or a school’s Intranet and Internet sites, employees’ access to the Internet, and the general usage by the employees of such facilities.

(Acknowledgements: This policy was drafted by Gary Brown, Stephen Corbishley, and David Emery of the Catholic Education Office, Diocese of Wollongong. The authors acknowledge the assistance given by the Department of Education State of Queensland, Wollongong City Council, and the CCER in preparing this policy.)

GENERAL PRINCIPLES

The computers and computer network facilities installed in schools, as well as the access facilities to e-mail, and the Internet are primarily for educational purposes, for the education of students. The usage of these facilities therefore must reflect and be consistent with that purpose. It is recognised that the facilities provide effective and convenient means for employees to communicate with each other, other educational professionals as well as accessing appropriate professional resources. Employees of the CEO and schools within the framework of this understanding may have access to these facilities as set down in this Policy on Acceptable Usage. These policies are developed for all employees, but apply automatically to all students, and therefore supervision of students will involve a strict adherence to this policy, and other policies that may be more restrictive of students’ use. Volunteers working in schools are included in the definition of employees and should be made aware of this policy.

CEO and/or school employees use of the Internet and Intranet from CEO and/or school accounts is governed by legislation, as well as any standards and guidelines of the CEO that may be in force from time to time. Employees are urged to be conscious of the principles in the idea of the Arena of Safety that their professional and personal behaviour particularly in respect of the use of electronic resources is consistent with that concept.

Further while legislation, standards and guidelines may not always explicitly refer to Internet/Intranet or e-mail use CEO and/or school employees should ensure that their use of and the manner in which they conduct themselves in this electronic environment does not contravene any law or standards or guidelines.

These standards must be uppermost in the mind of those employees whose responsibilities include the teaching and supervision of students accessing the electronic environment. The standard of supervision must reflect the principles in this document, and any employee who is in doubt about whether the standards apply or do not apply must consult with their co-ordinator or Principal.

Ethical Conduct
The principles relating to use of any CEO and/or school resource requires respect for the law, respect for persons, respect for the Catholic Church its mission and its values. It further requires integrity, diligence, economy and efficiency from the users of such facilities. All users of the CEO and/or school’s Internet and Intranet must conduct their activities in a manner compliant with the principles and expectations laid out in this document.

**Legal Requirements**

Complementing this document is any relevant legislation that may come into being from time to time. While the Freedom of Information Act (NSW) does not apply to the Trustees of the Roman Catholic Diocese of Wollongong at the time of this document being written, the principles which encompass all Internet and Intranet related activity, and the issues within the Freedom of Information Act are most relevant to Internet and Intranet usage.

For legal purposes e-mail has the same standing in court as paper documents. In addition employees must be aware that the CEO and/or schools can be involved in litigation and relevant records relating to use and activities in relation to e-mail, Internet and Intranet are "discoverable" by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of employees, parents, students or third parties as well as any relating to research, or other communications even if communicated in confidence.

‘Matters affecting personal affairs’ is the area most likely to be contravened by Internet and Intranet users. As such, users need to be particularly aware of the sensitivity of the material they access and disseminate.

Other legislation, which is particularly pertinent to Internet/Intranet applications, can include:

- Defamation Act (NSW)
- **Workplace Surveillance Act 2005 (NSW)**
- Copyright Act (Cth)
- Anti-Discrimination Act (NSW)
- Human Rights and Equal Opportunities Commission Act (Cth)
- Privacy Act (NSW)
- Crimes Act (NSW)
- Crimes Act (Cth)
- Telecommunications Act (Cth)
- Classification (Publication, Films and Computer Games) Act (Cth)
- Classification (Publication, Films and Computer Games) Enforcement Act (Cth)
- Classification (Publication, Films and Computer Games) Act (NSW)
- Classification (Publication, Films and Computer Games) Enforcement Act (NSW).

In addition, other legislation may be relevant, including

- Children (Care and Protection) Act) 1987

This list of legislation is not meant to be exhaustive. No reliance should be placed on the non-identification of a particular piece of legislation to support an inference that behaviour which may be prohibited or controlled under that non identified legislation, is implicitly or tacitly not forbidden by the CEO.

**CEO and/or school ownership of e-mail messages**
E-mail residing on or transmitted across a system is the property of the organisation that owns the system. This has the support of recent decisions in the Courts. All electronic files are therefore the property of the CEO and/or school and e-mail users should act on the basis that they can be and where necessary will be held accountable for every message issued from their machine, or authorised or issued on their behalf.

**Monitoring**

The CEO and/or school reserves the right to monitor any and/or all Intranet and Internet related activity undertaken by CEO and/or school employees, using CEO and/or school infrastructure, including, but not exclusively.

- activity relating to its Internet and Intranet sites
- activity relating to Internet access (see below)
- e-mail (see below)

**Internet Browsing**

CASTnet captures a record of all Internet Browsing and provides local school administrators and CEO administrators with the capacity to extract historical (current & previous month) reports for any user or user group. Such reports are generated by local Administrators on an intermittent basis as part of their review of Internet usage.

In addition to generating these reports, local administrators also receive reports providing the detail concerning any attempt to visit sites that are on the ‘blocked site’ filter list. Historical records of Internet browsing can be accessed at a systemic level.

All staff members need to be aware that they are subject to such monitoring of Internet use and ensure that they are acting at all times within the Acceptable Use Policy of the CEO.

**Email Usage**

CASTnet captures and stores records of email transactions that occur across its extended network. The logs include detail regarding date and time, sender, recipient and size of message.

If required for legal purposes, email content can be retrieved from archived media. In addition to SPAM and Virus scanning, email is also scanned for words that would be considered offensive. Messages containing offensive language that are 'sent' by users are in fact captured by the system and forwarded to the local Administrator for action in accordance with Acceptable Use Policy.

All staff members need to be aware that they are subject to such monitoring of email use and ensure that they are acting at all times within the Acceptable Use Policy of the CEO.

**ACCEPTABLE USE/issues**

Acceptable use issues are broadly categorised as personal conduct relating to:
CEO Wollongong Internet Usage Policy

- System security
- Legal requirements
- Ethical use of CEO and/or school resources
- Standards of interpersonal interaction in CEO and/or school employees’ or supervision of students’ use of electronic mail, access to the CEO and/or school’s Intranet and Internet sites, and employee access to the Internet.

**CONDUCT REQUIREMENTS**

CEO and/or school employees should abide by all of the following specific conduct requirements in their use of the Internet and Intranet, e-mail and other electronic communication devices:

**Summary of Requirements**

CEO and/or school employees should not purposely, in or by their use of CEO and/or school Internet/Intranet access and resources:

- Violate any State, Commonwealth or international law, or State or Commonwealth regulation, or fail to comply with CEO and/or school policies or procedures
- Violate generally accepted social standards, including netiquette, for the use of a publicly owned and operated communication vehicle
- Conduct any business or activity for commercial purposes or financial gain, including publishing material which contains any advertising or any solicitation of other network users or discussion group or list members to use goods or services
- Transmit or cause to be transmitted communications that may be construed as harassment or disparagement of others based on the criteria of the anti-discrimination legislation, defamation legislation and CEO and/or school policy.
- Download information or software from the Internet or Intranet for the purpose of providing to an unauthorised third party (eg games).
- Send via external e-mail or otherwise compromise proprietary, commercial-in-confidence, or sensitive information.
- Violate CEO and/or school or third party copyright, license agreements or other contracts
- Seek to gain unauthorised access to any resources within or outside of the CEO and/or school
- Disrupt or interfere with the intended use of the CEO and/or school’s Intranet and/or the global Internet and/or resources
- 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
- Compromise or without authorisation invade the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources
- Waste resources whether of peoples’ time, or the capacity of the system or the equipment;
- Post to a discussion group or other public forum personal communications without the author’s consent

**Personal Responsibility for Security**

System security is the individual and collective responsibility of all CEO and/or school employees
All suspected security violations should be treated seriously.

- CEO and/or school employees who suspect a security problem on the Internet or Intranet should;
  - immediately notify the Principal at school level or the consultant who may be nominated from time to time by the Director
  - not demonstrate the problem to others
- CEO and/or school employees who suspect their account has been tampered with should;
  - immediately change their password
  - contact the system administrator or Principal with specific details.

**Integrity of Computer-Based Information and Systems**

CEO and/or school employees must not in any way disrupt or interfere with the intended use of the CEO and/or school’s Internet and/or Intranet and/or resources

CEO and/or school employees must not without authority destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of computer based information and/or information resources, belonging to the CEO and/or school or to any other entity or individual, including, but not limited to, uploading or creating computer viruses.

**Development and Maintenance of Work-Related Skills**

CEO and/or school employees may use the Internet on personal time to practice Internet skills and explore Internet resources in order to develop or enhance work-related skills.

Personal time is defined as:

- Before and after work
- During lunchtime and other official breaks.

Appropriate activities include:

- Corresponding with colleagues and contacts around the world via electronic mail
- Connecting to resources that provide a variety of information
- Exploring the Internet looking for information resources useful in carrying out their duties.
- Diocesan based or authorised IRC and discussion groups.
- Other activity which may be defined as ‘cyberloafing’, that is the use of the organisations facilities and misuse of work time through accessing non related work sites is not permitted. In particular accessing sites that may be loosely defined as ‘pornographic’ is not an approved activity, and downloading from such sites is an abuse of the facilities provided.

**Use of e-mail**

**Privacy**

Electronic mail is not a secure medium, and even more so with e-mail sent via the Internet. Electronic mail is a CEO and/or school resource and is provided as a CEO and/or school communications tool. Staff with a legitimate purpose may have the need to view an
employee’s e-mail messages. Others may view e-mail messages inadvertently, since there is no guarantee of privacy for an electronic mail message. E-mail, along with other parts of the system, is regularly backed up and can therefore be preserved for some period of time on back-up tapes.

- CEO and/or school employees must not, without authorisation, invade the privacy of individuals or entities that are creators, authors, users or subjects of the information resources.
- CEO and/or school employees must not attempt to read another person's electronic mail or other protected files.

**Confidentiality**

The system administrator Principal or other employees of the CEO or school who, in the course of their work, have access to records, files, or data belonging to or about others including employees shall take precautions to avoid invading the privacy of individuals without their knowledge. These people must not divulge or disclose such information to others, unless required by CEO and/or school policy or State or Commonwealth law, and if required to disclose information must comply with the relevant guidelines in place relating to disclosure.

**Signature Block**

- CEO and/or school employees should attach a signature block containing the following minimum details to every Internet message and posting:
  - Name, Position, KLA (in secondary schools), Full name of the CEO and/or school, E-mail address, Work phone and fax. In addition each message must have as part of the signature block the phrase:
  - *Unless explicitly attributed the opinions expressed in this message are the personal views of the sender and do not necessarily represent the corporate opinion of the school, the CEO or the Diocese of Wollongong.*

**Publication of e-mail addresses**

- Where appropriate include e-mail addresses on official stationery, including compliments slips and fax sheets.
- CEO and/or school employees should include personal e-mail addresses on business cards, and on correspondence only where appropriate.
- CEO and/or school employees may provide personal e-mail addresses for inclusion in directories of office bearers of relevant professional organisations where they hold office in such organisations.
- Personal e-mail addresses for CEO and/or school accounts must not be included in personal listings such as the white pages of the telephone book.

**Personal security**

CEO and/or school employees should not reveal personal addresses or phone numbers, or personal addresses or phone numbers of other CEO and/or school employees in any e-mail communication.

**Listservs**

CEO and/or school employees
must not subscribe to Listservs concerned with purely personal interests, unconnected with the goals and purpose of their work unit or the CEO and/or school

should unsubscribe or suspend mail from Listservs for periods in which they will be absent.

should keep discussion, questions and comments relevant to the focus of the list.

should observe the common etiquette of the workplace and of the Internet in postings to Listservs

Unless CEO and/or school employees are formally and officially representing the CEO and/or school (as, for example, the CEO and/or school’s nominee on an inter-agency committee which is conducting its business wholly or partially through a special-purpose electronic discussion group) they must add the following disclaimer to their signature block when responding to a Listserv:

"Unless explicitly attributed the opinions expressed in this message are the personal views of the sender and do not necessarily represent the corporate opinion of the school, the CEO or the Diocese of Wollongong."

Newsgroups

CEO and/or school employees should not participate in Newsgroups concerned with purely personal interests, unconnected with the goals and purpose of the CEO and/or school

Chat

Employees of the CEO and/or school should not participate in Chat groups or sessions unless such session has been specifically set up to facilitate the communication between participants in a project or working group authorised by the CEO and/or school using CASTnet

Improper communications

• Improper communications are defined as chain letters or harassing mail.
  o Sending of improper communications by CEO and/or school employees may expose the CEO and/or school to risk of legal action or adverse publicity.
  o A CEO and/or school employee who receives an e-mail chain letter or a harassing message, should not delete it, and should immediately notify the Principal who will collect evidence to allow appropriate action to be taken steps to halt the communications and deal with the sender.

• Improper communications include ‘flamemail’. Flamemail is the use of e-mail to transmit offensive, insulting, harassing messages to other employees or persons outside the workplace.

Defamation

• CEO and/or school employees must not knowingly or recklessly publish, post or include in e-mail messages, material, which might be deemed to defame an individual, a company or an organisation.

Harassment

• CEO and/or school employees must not transmit, or cause to be transmitted, communications (whether in the form of text, picture or other data) that may be construed as harassment or disparagement of others based on the criteria of the anti-discrimination legislation and CEO and/or school policy. Staff are reminded that this
includes harassment or discriminatory behaviour based on age, gender, race, sexuality or disability.

- Staff may not engage in conduct or behaviour such as mounting personal attacks, including bullying, prejudicial or discriminatory attacks on others whether staff, students, parents, or those outside the school community.
- Users of screens must not upload or create ‘screensavers’ that are offensive to others, and may contribute to the creation of a hostile working environment to other employees.

Anonymous messages

- CEO and/or school employees must not send anonymous messages, defined either as messages that do not contain details of the sender’s name and affiliation, or messages sent through an anonymous e-mail service.
- CEO and/or school employees must not access non-school or non diocesan based e-mail systems, accounts eg Hotmail or other web based free e-mail services.

Conservation of Electronic Resources

- CEO and/or school employees should not wastefully use finite resources or obstruct the work of other CEO and/or school employees by consuming gratuitously large amounts of system resources (disk space, bandwidth) or causing congestion of the networks.
- Waste includes, but is not limited to:
  - Sending broadcast messages to lists or individuals.
  - Attaching files larger than 5mb to e mail messages
  - Unbridled and open-ended use of the Internet in terms of access time
- The content and maintenance of an account holder’s electronic mailbox is the responsibility of its owner. Messages received by the server are retained on the server until deleted by the recipient. CEO and/or school employees should actively conserve electronic resources by:
  - Keeping e-mail messages short
  - Checking e-mail daily
  - Deleting unwanted messages immediately
  - Keeping messages remaining in electronic mailboxes to a minimum
  - Down loading or extracting to files and then to disks mail messages required for future reference

Conservation of Print Resources

- Where it is necessary to update frequently consulted Intranet or Internet material CEO and/or school employees should make handwritten changes to paper documents rather than down loading and reprinting

Review of policy

The Director of Schools will review this policy from time to time.

Issue Date

October 2005
APPENDICES

Appendix 1

SCHOOL PUBLISHING ON THE INTERNET

CASTnet provides ALL schools the ability to publish on the Internet. While this ability affords considerable educational opportunity, the unregulated nature of the Internet requires that schools take care to maintain a safe and secure learning environment for all members of the school community. The requirements apply to all schools and all materials published by schools on the Internet using either the schools or any other Internet service.

School Publishing

Each school's 'home page' should include:

- acknowledgement that the school is a Catholic school under the management of the Diocese of Wollongong
- school contact details, which might include the school's postal address, phone and fax numbers and e-mail address.

Principal's Responsibilities

The Principal has responsibility for all material published in the school's name on the Internet.

Principals must:

- give written approval prior to the publication of all materials;
- ensure that all content is both appropriate for publication and of an acceptable quality;
- ensure that a process to regularly review and update all materials is developed and implemented;
- approve the inclusion of links to other Internet sites from the school's Web pages;
- ensure that all materials published in the school's Web pages have appropriate copyright clearance.
- this responsibility should not be delegated.

Privacy and Safety

Principals should ensure that the safety and privacy of students and staff is never compromised by materials published on the Internet. Therefore the following principles will apply in all circumstances:

Personal and private information about students or staff, such as home telephone numbers or addresses, or private e-mail addresses should never be published.
Written permission is required from a parent or guardian prior to the publication of any material by or about any student, including photographs of students.

Schools should take great care with the publication of student photographs. Individual photographs of students should not generally be published. Students depicted in class or group photographs should not be identified individually by name.

To maintain a degree of anonymity, students and students' work should be identified by Christian or given names only. Schools should carefully consider the implications of publishing the full names of students.

Where schools wish to publish information about staff (such as names, photographs, classes taught, or school e-mail addresses) written approval is required from each staff member involved. Staff may choose not to have their information published.

Students should not be provided with individual e-mail access; class or group e-mail mailboxes will suffice in most instances. The Principal, however, may make exceptions for responsible students in specific circumstances. The use made of individual student e-mail access should be monitored carefully and reviewed regularly.

An appropriate staff member should monitor e-mail messages to and from class or group e-mail mailboxes to ensure the safety of students is not jeopardised.

Where schools choose to provide links to other Internet sites from their Web pages an approval and review process should be incorporated to ensure that these links are, and remain, educationally appropriate. A warning indicating the transient nature of Internet material and sites should be associated with the links.

**Appendix II**

**Suggested Internet and Electronic Mail Permission Form**

[The school] is pleased to offer students of access to the computer network for use of the e-mail and Internet. To gain access to e-mail and the Internet, all students under the age of 18 must obtain parental permission and must sign and return this form to the [Put Name Here]. Students 18 and over may sign their own forms.

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases, and other information sources while exchanging messages with Internet users throughout the world. Families are warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, (parents and guardians of minors) are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, [School Name] support and respect each family's right to decide whether or not to apply for access.

**School Internet and e-mail Rules**
CEO Wollongong Internet Usage Policy

Students are responsible for good behaviour on school computer networks just as they are in a classroom or in the playground. Communications on the network are often public in nature. General school rules for behaviour and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege - not a right. Access entails responsibility.

Network storage areas should be treated like school lockers. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on school servers would be private.

During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

As a user of the school network and the Internet, students must acknowledge and agree that the following are not permitted:

- Sending or displaying offensive message or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using another’s password
- Trespassing in another’s folders, work or files
- Intentionally wasting limited resources
- Employing the network for commercial purposes

Violations may result in a loss of access as well as other disciplinary or legal action.

Appendix III

User Agreement and Parent Permission Form - 2005

As a user of the [School Name] computer network, I hereby agree to comply with the above stated rules communicating over the network in a reliable fashion while honouring all relevant laws and restrictions.

Student Signature:

Homeroom:

As the parent or legal guardian of the student signing above, I grant permission for my son/daughter to access networked computer services such as e-mail and the Internet. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable. I note the school will endeavour to ensure students will not come into contact with such material but I accept responsibility for guidance of my children in use of the Internet. In particular I will seek to support the school’s standards and in addition set and convey standards for my daughter or son to follow when selecting, sharing or exploring information and media.
Appendix IV

Notice to Employees of the Catholic Education Office, Diocese of Wollongong pursuant to s10 of the Workplace Surveillance Act 2005 (NSW).

This Notice is provided pursuant to the provisions of the Workplace Surveillance Act 2005 (NSW). In accordance with the Policy on the Acceptable Use of the Internet, Intranet, e-mail and other Electronic Communication Devices ("the Policy") employees are advised that their Internet and email use may be monitored by system administrators and others, as nominated by the Principal or CEO or by third parties nominated by the CEO. Computer surveillance is currently operative, it is continuous and ongoing. By logging on to the network, you acknowledge that you have read and understood this Notice and the Policy. The Policy on the Acceptable Use of the Internet, Intranet, e-mail and other Electronic Communication Devices may be accessed at www.ceo.woll.catholic.edu.au/policies/internet.pdf

Gregory B Whitby

Director of Schools