1. RATIONALE AND PURPOSE

The nature of the work of office and school based employees of the Catholic Education Office (CEO) in the Diocese of Wollongong is entirely embedded in the delivery of high quality educational services to students enrolled in our Catholic schools. The use of Information and Communication Technologies (ICTs) contributes to the broadening and availability of learning and teaching options and enhances the efficiency and effectiveness of educational administration and policy.

The general principles underpinning this policy are to:

- Maintain an ethical, safe and supportive working and learning environment
- Instruct employees in making informed decisions about the use of ICTs
- Ensure the privacy and protection of our employees and students
- Remind employees about the right of the CEO to access CEO computers, network, internet logs and email for various purposes including auditing, forensic data gathering, planning and fault determination
- Ensure appropriate accountability is in place to monitor use of ICTs
- Ensure that ICTs in the workplace are not used improperly or illegally.

This policy sets out the basis upon which all employees are able to use the ICT facilities provided by the employer and the acceptable use of personal ICTs when interacting with others in what can reasonably be perceived as a work related context. The use of ICTs in this context is to be consistent at all times with the Vision and Mission Statement and the General Principles of Employment under which all employees are engaged. The policy confers certain privileges on employees and details their responsibilities in relation to both official and personal use of CEO resources.

1.1 SCOPE OF THE POLICY

This policy relates to the use of computers, mobile phones, any associated networks or networking equipment, corporate systems including email systems and emerging technologies and applies to all employees (including volunteers) and contractors of CEO schools and offices.

It is not intended to be exhaustive and cannot anticipate all current and future uses of ICTs. If any employee is unsure about interpreting this policy, he/she is responsible for discussing this with the Principal or Head of Service as soon as possible.
The CEO expects users to make responsible choices when using ICTs and attempts to ensure employees understand the implications of their choices. Responsibility for appropriate use of the technologies lies with the user.

2.0 **PROVISION OF ICT TO EMPLOYEES**

- All ICT devices that are provided to employees remain the property of the CEO or school. They are allocated to the employee to assist in the execution of the duties their position requires.

2.1 **EMAIL AND INTERNET**

- All employees in CEO offices and schools are provided with an email address and access to ICT while at work.
- The CEO provides a secure private network with secured proxied connections to the internet.
- No school connects directly to the internet.
- The CEO wide area network, in conjunction with services offered by CEnet, is provided for use by staff and students. Remote access to this network is provided by access solutions managed and maintained at the CEO.
- This access is issued at the discretion of the Principal/Head of Service as required by the specific position duties.

*Email accounts will be maintained for three months after the departure of an employee, but will only be accessible by the CEO.

2.2 **COMPUTERS**

- Where a staff position at the CEO or school is deemed to require access to a computer (laptop or desktop) that position will be provided with a suitable computer. The type of computer required will be determined by the Head of Service in conjunction with the ICLT team. Where required, access to the CEO computer network and internet for staff, will be made available as deemed as appropriate by the above mentioned parties.

2.3 **MOBILE AND SMART PHONES**

- Where a staff position at the CEO is deemed to require access to a mobile telephone that position will be provided with a suitable device. In the case that a Smart Phone is required for the use of enhanced messaging and collaboration features, the type of Smart Phone will be determined by the management of the section the position is in, in conjunction with discussions with the ICLT staff. Where required, access for
staff will be made available via the phone to the CEO/school computer network and internet as appropriate.

- Each employee is required to check the phone bill and report any discrepancies as well as reimburse the CEO/school for personal use of the phone. In general, costs should not exceed the cap placed on the plan that has been issued with the phone. Employees should note that mobile data is unfiltered and should be treated with extreme care.

2.4 PERSONAL RESPONSIBILITY FOR ICTS

- Employees must maintain password security on school/CEO devices and either lock their computer screen or log-out when they leave their work area to avoid unauthorised access to confidential information.

- Portable ICTs have been asset registered and each employee is accountable for all of the hardware and peripherals that have been supplied. These ICTs must be returned for auditing purposes as requested, when on extended leave and at the conclusion of employment.

- Employees are responsible for the security of devices supplied to them by the CEO/school at all times.

- Portable ICTs should not be left in vehicles from both a security and possible damage perspective (due to ambient heat). If this is occasionally unavoidable for a short period of time, the device must be locked in an appropriate compartment/boot, out of public view.

- Insurance policies are in place to cover accidental damage, loss or theft of devices whilst on CEO/school premises. All claims of loss or theft will be subject to investigation by CEO internal audit or Catholic Church Insurances, to ensure that malicious damage or a willful breach of policy has not occurred. All damages, loss or theft must be reported within 24 hours (or as soon as possible thereafter) to the police where necessary and to the Principal/Head of Service. Employees may be required to pay insurance excess in the case of negligent care of devices.

- The employee is responsible for all electronic mail originating from their account. All email remains the property of the CEO/school.

3.0 ACCEPTABLE USE

The CEO/school includes activities such as (but not limited to) the following as acceptable use of ICTs:

- Facilitating, gathering and disseminating information for work related projects
- Encouraging collaborative projects and resource sharing
- Fostering innovation in the workplace
- Building broader infrastructure in support of education and research
• Fostering professional development
• Undertaking administrative functions that support the school or office.

3.1 WHAT IS WORK RELATED USE?

Work related use of ICTs includes (and is not limited to) the following:
• Accessing curriculum related information and resources
• Administration and administrative support
• Research for educational or administrative purposes
• Support of student welfare and pastoral issues
• Addressing professional and educational issues
• Professional and cordial communication with inter-school and external work colleagues and stakeholders
• Accessing employment related information for example, Work Health and Safety, union information etc.
• Communication with students in a manner consistent with their role and responsibilities and in relation to educational/school/CEO matters.

In general CEO/school provided ICTs are for business and educational purposes and all employees have a responsibility to ensure their proper use. ICTs are a valuable resource and employees are required to use them efficiently, economically and ethically at all times. As with any other work related activity, employees must not engage in any use of ICTs that may be considered questionable, controversial or could potentially damage the reputation of the school, CEO or the Church (also refer to the Code of Conduct in the Protection of Children and Young People).

3.2 WHAT IS UNACCEPTABLE USE

Employees must not use ICTs for any of the following:
• Abuse, threaten, vilify, defame, harass or discriminate against others
• Send or receive obscene, pornographic or child abuse material
• Uploading, downloading, sending, circulating, displaying or responding to any of the following materials:
  o Sexually related, pornographic or child abuse material or messages containing thoughts and feelings with overly familiar or sexual connotations
  o Violent or hate-related messages or material
  o Threatening, defamatory, obscene or harassing messages or material
  o Racist or other offensive messages or material
  o Subversive or other messages or material related to illegal activities.
• Injure the reputation of or embarrass the CEO/school
• Spam, unauthorised mass mail or send or receive chain mail
• Loading of unlicensed or unapproved software
• Infringing the copyright or other intellectual property rights of another person (in particular, but not limited to, copyrighted music and video files)
• Perform any other unlawful or inappropriate act
• Unauthorised copying of programs and systems files
• Accessing social networking sites for personal use
• Allowing open network shares on computers
• Unauthorised connection of non CEO/school computer or network attachments to the CEO or school network
• Unauthorised use of another employee’s password
• Connecting directly to the Internet through a bypass of CEO/school and CEnet managed services
• Use of remote access services other than the CEO/school provided services such as the use of unauthorised online anonymous proxy servers
• Forgery or attempted forgery of electronic mail messages
• Reading, deleting or modifying the electronic mail of others
• Personal profit or gain.

Comments that are not appropriate in the workplace will also be inappropriate when sent by email, SMS or via other messaging. These messages can be easily misconstrued and so employees must exercise good judgement and so choose their words carefully and express themselves in a clear and professional manner.

3.3 SOCIAL NETWORKING

• An employee of the CEO/school needs to be a role model, mentor, and advice giver – not a ‘friend’ to students and their families. When a student gains access into an employee’s network of friends and acquaintances and is able to view their personal photos and information, the professional dynamic is significantly altered.

• Social network sites like Facebook and MySpace easily blur the relationship because of the personal information made available on profiles and the links to other parts of the digital footprint of the employee.

• Ultimately, sites like Facebook are social environments. CEO and school employees must operate in a professional capacity, therefore being social with students or their families in private social network spaces, introduces a dynamic that may place both parties at risk; not necessarily because the relationship is inappropriate but because the relationship could be perceived in that way. **Therefore any private communication with students creates a high risk situation for employees.**

• Employees are expressly prohibited from accepting or inviting students as ‘friends’ on personal social networking sites. It is important to recognise the difference between ‘My Classes’ and other publically accessible social network sites. Employees must speak with their Principal/Head of Service if they require any clarification.

3.4 PERSONAL USE

• Employees are permitted to use CEO/school provided ICTs to send and receive personal messages and for very limited personal purposes (e.g. occasional internet banking) provided that such use is kept to a minimum and does not interfere with the performance of duties, particularly the supervision of students. However it is
important to note that such personal use is subject to the same terms and conditions of this policy.

3.5 WORKLOAD

- There is a real potential for the use of ICT services to impact upon the workload of employees during and after formal hours of work. It is recommended that email in particular be responded to in a reasonable and orderly fashion, prioritising urgent matters and using an ‘away message’ or other automated response message as required.

- Employees are not required to be accessing and responding to work related email or other messaging technology at all times of the day or night and should plan a period of time at the commencement and conclusion of the working day for undertaking this task.

- Each school needs to advise parents of its expectations of using emails to communicate with staff and the fact that response times may vary. Urgent matters must be directed by phone to the school office.

4.0 CEO MONITORING AND AUDITING

- Electronic information including email and files stored on the CEO equipment and network resources are considered to be an open record, much like a written or printed document, and can be requested for audit at any time. The CEO/school reserves the right to review outgoing and incoming email sent to or from the CEO/school email program.

- Electronic information including email and files may also become available to others under the following circumstances:
  - Software or hardware failure
  - User error or misconfiguration
  - Network administrator may have access to data while:
    - Performing routine operations or pursuing apparent streams or user problems.
    - Protecting the integrity of the CEO ICT system and the rights and property of the CEO.
    - Protecting the rights of individuals working in collaborative situations where information and files are shared
    - Where there are grounds to suspect a breach of this policy
  - In random, ongoing and continuous checking processes of employee use pursuant to employer rights under the Workplace Surveillance Act 2005. Employees are notified through this policy and each time they log on to the CEO/School network which they must acknowledge to have read and accepted. This monitoring is undertaken by the Principal and his/her nominated staff, the CEO or other nominated third parties.
• The Network Administrator is required to report apparent improper or illegal activities that they discover to the Chief Technology Officer. Breaches of policy or potentially illegal use will be referred to Human Resource Services, and as required to the Police, for further investigation. No guarantee of complete privacy is made or implied in the provision of ICTs to employees by the CEO/school.

• For legal purposes email has the same standing in court as paper documents and can be “discoverable” by way of court order or subpoena in a range of matters that can be brought against the CEO or the employee.

5.0 BREACHES OF THE POLICY

ICT resources provided to employees are a valuable and limited resource and the CEO/school expects that they will be respected according to this policy. Should this not be the case any proven breaches of this policy can result in, but is not limited to, any one of the following:

• Loss of individual access to systems
• Loss of individual access to various ICTs
• Disconnection of entire sites from the CEO network
• Appropriate administrative sanctions and disciplinary action
• Summary Dismissal, subject to the appropriate process
• Notification to an external agency
• Criminal charges. Or legal proceeding in accordance with State and Federal legislation.

Employees must report any suspicious SMS, MMS, email or use of ICTs that may be in breach of this policy to the Principal /Head of Service. Any such messages or record of use must not be deleted as they may be required for investigation purposes. Failure to report may result in the employee being held accountable for the breach.

OTHER RELATED POLICIES, GUIDELINES and LEGISLATION

Policies
Vision and Mission Statement
General Principles of Employment
Code of Conduct in the Protection of Children and Young People
Staff Relations Policy

Legislation
State Records Act 1998 (NSW)
Defamation Act (NSW)
Workplace Surveillance Act (NSW)
Copyright Act (Cwlth) and Copyright Amendment (Digital Agenda) Act 2000
Anti-discrimination Act (NSW)
Privacy Act (Cwlth) and Personal Information Protection Act 1998 (NSW)
Crimes Act (NSW) 1900 (Cwlth) 1914
Telecommunications Act (Cwlth) 1997 and Associated Acts
Broadcasting Services Act 1992 (Cwth)
State and federal Anti-discrimination legislation

IMPLEMENTATION AND REVIEW

All Principals and Heads of Service are responsible for the implementation of this policy in their respective areas.

The ICLT Manager is responsible for regularly reviewing the practical application of this policy and advising the Head of Human Resource Services of the need for modification to any aspect of the document.

All new employees must be provided with a copy of this policy as part of their induction information package.

Version Control and Amendment History

<table>
<thead>
<tr>
<th>Version Control</th>
<th>Date Approved</th>
<th>Approved by</th>
<th>Amendment</th>
<th>Review Date</th>
</tr>
</thead>
</table>
| 1.0             | 25/10/2011    | Carolyn Hadley  
*Head of Human Resource Services* | New policy. | December 2012 |
| 1.1             | 14/01/2013    | Carolyn Hadley  
*Head of Human Resource Services* | Slight grammatical changes. | December 2014 |
| 2.0             | 10/12/2014    | Carolyn Hadley  
*Head of Human Resource Services* | Additional wording and slight grammatical changes. | December 2015 |