ICT Acceptable Use Policy

UPDATED MARCH 2014

RELEVANT TO	Diocesan Personnel, Contractors, Volunteers and any user of ICT systems and equipment (Includes all agencies and Parishes except the CSO)
INTRODUCED	Drafted: 01/07/2002, Published 2009
REVIEW DATE/S	14/03/2014
APPROVED BY	Diocesan Executive – 19/03/2014
RELATED POLICIES	Diocesan Social Media Policy (2013)
RELATED FORMS	
SPONSOR	Manager, ICT Services

1. Aim

The Diocese of Maitland-Newcastle (the Diocese) has a responsibility to protect users, clients and Diocesan resources from illegal or damaging actions by individuals committed either knowingly or unknowingly.

The acceptable use policy provides guidance on how the Diocesan information and communication technology (ICT) infrastructure shall be used to facilitate effective information management.

2. Purpose

This policy sets out the responsibilities for all ICT users of the Diocese, regarding the proper and permitted use of the network, including Internet, email and web browsing.

"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." p. 1 Australian Privacy Commission 2001.

3. Scope

This policy applies to permanent and temporary employees, contractors, consultants, volunteers and all other users of ICT systems of the Diocese and its relevant agencies, being the CDF, Pastoral Ministries, Finance and Administrative Services, CatholicCare and the parishes.

This policy applies to all equipment that is owned or operated by the Diocese. All users are urged to ensure that their professional and personal behaviour in relation to email and web use is consistent with this Policy. Unacceptable use of the network and breaches of this Policy may require disciplinary procedures.

Note: The Catholic Schools Office (CSO) and its connected networks are not included within the scope of this policy. Please refer to the CSO policy on Internet Email and Network Usage in the workplace, however the use of Diocesan resources by CSO staff

4. Responsibilities

All users	Fully understand the implications of the acceptable use policy; ensure that use of Diocesan ICT resources is in accordance with the policy
Heads of Diocesan agencies	Approve the content of acceptable use policies; promote awareness of this policy and implications for breaching this policy; take disciplinary action where policy breaches are identified
ICT Services Team	Ensure all users are aware of and agree to the acceptable use policy when access is granted to the Diocesan network; monitor the use of the network and report policy breaches to the Head of Agency where appropriate
Managers	Ensure that direct reports have signed a copy of the policy and that it has been placed in their file.

5. Policy

Usage

The Diocese provides computers and Internet access to support the mission of the Church and the administration of the Diocesan Agencies, and to enhance the opportunities for Diocesan staff. All ICT equipment remains the property of the Diocese or its agencies.

Users are to utilise Diocesan computers, networks and Internet services for work-related purposes. Incidental personal use of Diocesan 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 user for occasional personal communications. Users are reminded that such personal use must comply with this Policy and all other related procedures and rules.

Users are expected to use appropriate judgement and caution in communications concerning individuals and staff to ensure that personally identifiable information remains confidential.

Privacy expectations and intellectual ownership

Users may not be aware that their browsing activities, email & instant message content as well as call records can be scrutinised. System administrators are able to access user's data and log network and communication use as part of their role.

In reviewing and monitoring user accounts and information, the Diocesan systems administrators will respect the privacy of individuals. These people must not divulge or disclose such information to others unless required by the Head of Diocesan Agency, the Head of Human Resources, or State or Commonwealth Law. (Ref. National Privacy Principles 2001). If during the course of their duties a system administrator discovers information that demonstrates a breach of this policy, information

about this breach will be reported to the Information & Communications Technology Manager, who will be responsible for liaising with the respective Head of Diocesan Agency or Head of Human Resources. In the event that a breach has been committed directly by a Head of Diocesan Agency the matter will be referred directly to the Bishop.

System administrators within the Diocese include the Bishop, Information & Communications Technology Manager and delegated personnel as specified by the Bishop or the Information & Communications Technology Manager.

Materials produced, sent and kept by employees, remain the property of the relevant Diocesan Agency of the Diocese of Maitland-Newcastle.

Electronic mail

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
- Emails are hard to destroy. Even deleted emails are backed up and recoverable
- 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 Diocesan network. (www.privacy.gov.au).
- The Diocese reserves the right to block any email message suspected to contain a virus or other inappropriate content.

Acceptable use of email in the workplace

Acceptable use of email is defined as communication to others on work-related matters, connected with the goals and purposes of each respective Diocesan Agency.

Unacceptable use of email in the workplace

Unacceptable use is where email is used to:-

- Distribute unsolicited email messages, including "junk email" or "spam" or other advertising materials, except in the case of diocesan agencies sending material of an advertising or promotional nature to users within the Diocesan system.
- Use Diocesan email distribution lists without authority, or for the sharing of non-work related matters
- Harass or discriminate other users
- Flame (send abusive email)
- Defame other employees, the Diocese, or another individual or organisation
- Disclose personal information or contact details about another employee
- Receive, maintain or transmit pornography
- Read another person's email or other protected files

- 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
- Unauthorised use, or forging, of email header information
- Access non-Diocesan based email systems or accounts. e.g. Hotmail, Gmail or other email services. These externally provided systems cannot be guaranteed to have provided acceptable protection against viruses and other malware
- Waste resources - time, or the capacity of the system or the equipment. This is especially inappropriate for personal use, or where productivity is directly affected
- 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
- Send sexually explicit, suggestive, or other harassing material
- Distribute information that could reasonably be regarded as misleading and represents a conflict of interest with the organisation.

Internet access and web browsing

Logs are maintained that record information on the sites which people visit. The keeping of these logs is necessary for the routine maintenance, security and management of networks and systems. Information is logged automatically.

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.

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 (www.privacy.gov.au).

All users have a dual responsibility to protect those in their care e.g. clients, school students, or elderly residents, from offensive material, and to ensure that no one may be liable for transmitting offensive material.

The Diocese reserves the right to restrict access to any Internet site suspected to contain a virus or other inappropriate content.

Appropriate use of the Internet in the workplace

Acceptable use of the internet is defined as accessing information and resources for work-related matters, connected with the goals and purposes of each respective Diocesan Agency.

Unacceptable use of the internet in the workplace

Unacceptable use is where the internet is used to:-

- Download sexually graphic material
- Access web sites that contain pornographic material
- Participate in 'Chat Groups' or use other chat/instant messaging technologies for discussions 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 unnecessary information or unauthorised software
- Violate Diocesan or third party copyright or licensing agreements or other contracts
- Seek to gain unauthorised access to any resources within or outside of the Diocese
- Waste resources - time, or the capacity of the system or the equipment. This is especially inappropriate for personal use
- Access sexually explicit, suggestive, or other harassing material

Use of Social Media

Use of social media, whether in a personal capacity or as part of a role within the Diocese, must be carried out in line with Diocesan Social Media Policy (2013)

Use of ICT resources

The following guidelines exist on the general use of Diocesan computer and network facilities in general:-

- Users must not make contact through any form of information technology with children or young people whom you know through your role in the Diocese for any relationship or contact outside your professional role, unless such contact has prior approval from a manager
- Users must not make contact with children or young people via any form of information technology for the purpose of initiating or maintaining an inappropriate relationship
- Extensive use of the network or other ICT resources 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 disclose their account details or passwords to any other person.
    - Users will maintain passwords that would not be easy for someone to guess and will change their password regularly.
    - Users will log off or lock their workstations when unattended and set a password protected screensaver to prevent unauthorised use of their computer and credentials

- 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 hardware and software components of a computer or computing system is prohibited. This includes the introduction of malicious programs into the network or server including but not limited to viruses, worms, Trojan horses, e-mail bombs
- The installation of unlicensed software for use on Diocesan computers is prohibited
- The Diocese reserves the right to monitor the use of any Information Technology or Communications resource. Monitoring will be conducted in accordance with the NSW Workplace Surveillance Act, 2005. Users should be aware that acceptance of this policy constitutes official notice that surveillance may be conducted under the Act
- Diocesan ICT resources must not be used to conduct illegal activities as defined by any legislation, including but not limited to the Australian Commonwealth Government Act, 1989
- Diocesan ICT resources must not be used to access any material which would be considered offensive or derogatory on the basis of race, sex or religion; and which a reasonable person would deem unacceptable.

Use of Mobile ICT resources

The Diocese provides mobile ICT equipment and resources to users who have roles that require them to be contactable when working away from their normal base, who regularly travel between sites or who are on-call after hours.

Users must be efficient, economical and ethical in their use and management of these resources which are provided for organisational purposes. All employees have a responsibility to ensure the proper use and security of these resources in line with the rest of this policy.

Additional responsibilities particular to mobile and portable devices include:

- Physical Security. Mobile ICT equipment should be secured at all times to prevent damage or theft
- Safe Operation. Mobile ICT equipment should not be used while controlling a vehicle or other machinery. This goes beyond the road rules that condone some hands-free usage as it has been shown that having a mobile phone conversation (regardless of using hands-free technology) while driving can increase the risk of a crash resulting in hospitalisation by four times (*BMJ, 2005*).
- Return of Equipment. All mobile ICT equipment must be returned to the Diocese or its agencies on cessation of a user's engagement.

Consequences of inappropriate behavior

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. If so,

a thorough and transparent investigation of the alleged breaches will take place. This investigation will be carried out by the Head of Diocesan Agency and/or his/her delegate.

Failure to comply with this Policy governing computer use may result in disciplinary action, up to and including dismissal. Offenders may be disciplined via the relevant Diocesan Agency disciplinary procedures, which may include termination of their employment. Illegal uses of the Diocesan computers will also result in referral to law enforcement agencies.

In the case of accessing child pornography, police will be notified of the offence. The NSW Crimes Act 1900 Section 578B lists possession of child pornography as an offence that may involve child abuse. If a user is found to be accessing child pornography sites or in possession of child pornography, the matter will be reported to the police and the NSW Ombudsman. (Section 3.1.5 NSW Ombudsman Child Protection: responding to Allegations of Child Abuse Against Employees requires that misconduct that may involve child abuse must be investigated and reported to the Ombudsman).

Acknowledgements

The following resources were used in the preparation of this policy document:-

- Procedures for the Acceptable Use of the Internet and Email, The Catholic Education Office, Diocese of Wollongong
- The Australian Privacy Commissioner's Website 2001 Update
- Employment Relations News, Volume 2 April 2001, Australian Catholic Commission for Employment Relations (ACCER)
- Catholic Education Commission Web Site - Copyright, Internet & Email Use
- NSW Ombudsman Child Protection Act 1974
- NSW Workplace Surveillance Act 2005
- CCER Newsletter Vol 4 No 9, 10th August 2005
- CCER sample Staff Email & Internet policy September 2005
- British Medical Journal, http://www.bmj.com/content/331/7514/428

Review and acceptance

In order to ensure that all users are aware of their obligations under this acceptable use policy, all users shall be required to review and accept this policy prior to accessing any ICT resources. In some cases, the policy will be displayed on user logon and need to be accepted to gain access to the computer. In this event the date of acceptance is recorded in the central ICT Active Directory.

The policy should also be reviewed as part of Induction.

The use of ICT resources constitutes acceptance of this policy.

Revision History

Date	Author	Description of Changes
01/07/2002	Various	Initial version – published on the Diocesan website
06/10/2004	Brendan Klasen	Reviewed and adjusted policy to fit Diocesan ICT information security templates
11/07/2005	Brendan Klasen	Updated Child Protection Policy wording; Released for comment to heads of Diocesan agencies
15/08/2005	Brendan Klasen	Updated with feedback from heads of Diocesan agencies. Forwarded to the Bishop for final approval

13/09/2005	Brendan Klasen	Updated with further revisions from heads of Diocesan Agencies. Released for final review and comment
27/09/2005	Brendan Klasen	Updated with content for Workplace Surveillance Act 2005. Policy accepted by Heads of Diocesan Agencies
03/11/2005	Brendan Klasen	Modified scope to exclude Catholic Schools Office
19/12/2005	Brendan Klasen	Approved by the Bishop's Executive Committee for release
12/12/2008	David Butterworth	Reviewed policy with no changes required
18/5/2009	Jo Hanlon	Policy format updated Reviewed by DOMN Exec and published
15/01/2010	David Butterworth	Corrected ICT from ITC
07/02/2012	David Butterworth	Added responsibility of "Managers" Added references to Instant Messaging and locking of workstations
08/01/2014	David Butterworth	Updated to current documentation style Added references to Social Media Policy and various minor updates Incorporated items specific to mobile ICT equipment
19/03/2014	David Butterworth	Approved by Diocesan Executive