

	ACCEPTABLE USE OF ICT RESOURCES	Document No:	ICT-PRO-005	
		Approval Date:	4/08/2020	
		Approved By:	M. Willett	
		Review Date:	4/08/2022	
		Responsible Officer: Digital Strategy Manager	Expiry Date:	N/A
		Authorising Officer: Chief Operating Officer	Issue No:	4/08/2020

1. Purpose

The Australian Catholic Bishops Conference (Conference) provides information and communication technology (ICT) resources to workers to assist them to conduct their work efficiently and effectively. Users of Conference's ICT resources have a responsibility to ensure that their use of these resources is legal, ethical and complies with the Conference's aims, objectives and values.

This document provides guidance on the requirements for appropriate and efficient use by Conference workers of Conference's ICT resources.

2. Scope

The guidelines stated in this document apply to workers at all Conference agencies. It is an expectation that all workers will comply with these guidelines.

3. Related Documents

State and Territory WHS Legislation
 State, Territory and Commonwealth Antidiscrimination Legislation
[ACBC Use of Information Technology Systems Policy](#)
[ACBC Privacy Policy](#)
[ACBC Website Privacy Policy](#)
[HR-PRO-036 Sexual Harassment](#)
[HR-PRO-011 Grievances](#)

4. Definitions

Electronic communications

Electronic communications include World Wide Web sites, electronic mail (email), instant messaging and any other material sent electronically.

Conference's ICT resources

Conference's ICT resources include Conference's and its agencies' networks, system software and hardware, any Conference's intranet, extranet, mail systems, computer systems, software, servers, desktop computers, printers, scanners, portable computers, tablets, leased notebook computers, mobile telephones, portable storage devices including digital cameras and USB memory sticks, hand held devices (for example personal digital assistants or PDAs) and other ICT storage devices.

Copyright material

Copyright material is material belonging to a third party which includes (but is not limited to) software, database files, documentation, cartoons, articles, graphics, text and downloaded information.

ICT use

ICT use is all aspects of the use of Conference's ICT resources including:

- publishing and browsing on the internet;
- downloading or accessing files from the internet or other electronic sources
- email
- electronic bulletins/notice boards
- electronic discussion/news groups
- weblogs ('blogs');
- social and professional networking (e.g. use of Facebook, Myspace, Twitter)
- LinkedIn
- YouTube
- file transfer
- file storage
- file sharing
- video conferencing
- streaming media
- instant messaging
- online discussion groups and 'chat' facilities
- subscriptions to list servers, mailing lists or other like services
- social commerce posting, like product or experience reviews
- copying, saving or distributing files
- viewing material electronically
- printing material
- Other electronic devices

Malware

Malware is an abbreviation of "malicious software" and means software programs designed to cause damage and other unwanted actions on a computer system. Common examples include computer viruses, worms, spyware and Trojans.

Offensive or inappropriate material

Offensive material is material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually orientated messages or images and messages that could constitute sexual harassment.

Child

Any person under the age of 18.

Personal information

Personal information can include photographs and images, addresses and telephone numbers, information about a worker's hours and place of work, in-house procedures or routines, or anything else that could compromise individual and collective staff safety or that of Catholic entities.

Personal use

Personal use is all non-work-related use and includes internet usage, SMS, MMS and private emails.

Users

Users are all workers who use email, internet and other electronic communications provided by the Conference, either during or outside working hours, including the use of remote access facilities.

5. Responsibilities

Agency Heads

Agency Heads are responsible for ensuring that:

- Induction of new workers includes these guidelines and the ACBC Use of Information Technology Systems Policy
- All workers are made aware of the meaning of acceptable use of ICT resources
- Their agency complies with all legal requirements (e.g. privacy, security, discrimination, etc.)

- Breaches of acceptable use are addressed in a timely manner and in accordance with standard procedures

ICT Functions

The ICT functions (where they exist) in Conference agencies are responsible for:

- Advising on the acceptable use of ICT resources
- Implementing and maintaining any systems that assist in compliance with acceptable use
- Compliance with State and Territory law in relation to monitoring or surveillance of ICT use

6. General Principles of ICT Use

1. **Be accurate, truthful, respectful and considerate in your posts**
Workers should be constructive, provide appropriate context, and think about the impact of their comments on the Conference, other workers, external bodies and the Catholic community. Words matter, especially when Conference workers discuss topics that may be controversial.
2. **Take responsibility for your words**
The Conference will hold workers personally accountable for comments deemed defamatory, obscene, or libellous in their Agency Head's reasonable opinion, whether they pertain to the Conference, another organisation or another person.
3. **Assume that anyone can see what you post**
The internet is fully searchable, which means that anyone with an internet connection, including your employer, your colleagues, children, vulnerable people and other members of the public, can find even the most obscure information.
4. **Safeguarding**
Workers should ensure that any communications with children or vulnerable adults is transparent. Where possible direct communication with individual children via internet, email or social media should be avoided and should be through an intermediate such as a school, parish or other organisation.
5. **Monitor your use**
Workers should ensure that personal use of Conference's ICT resources does not interfere with Conference work commitments.
6. **Be safe**
Workers should be careful about posting personal information online, whether it is information about themselves, other workers or anyone else.
7. **Maintain security of the networks**
The Conference makes its ICT resources available to workers on the understanding that they observe any guidelines to protect the security of the systems.

7. General Responsibilities of Conference and Users of ICT Resources

1. As the owner of the Conference's ICT resources, the law can hold the Conference vicariously liable for its improper usage. In light of the substantial legal obligations, the Conference as the employer is responsible to take all reasonable steps to ensure appropriate usage of the network and to monitor user compliance with these guidelines.
2. Although the Conference cannot guarantee the protection of individuals against the existence or receipt of material that may be offensive to them, it undertakes to take every reasonable attempt to protect them against invasions of privacy and other possible dangers associated with the use of the organisation's computer and electronic communication networks.
3. It is the responsibility of the Conference as the provider of the electronic communications to ensure that users receive:
 - Training on these guidelines
 - Regular and timely advice about these guidelines
 - Updates and amendments to these guidelines if and when they occur

4. By using Conference's ICT resources, users acknowledge their responsibility to comply with the principles and requirements outlined in this procedure and understand the consequences of breaching the Conference's Use of Information Technology Systems Policy and this procedure.

8. Safeguarding

It is a fact that while technology can be used for much good in keeping people in contact with one another, it can also be an instrument through which great harm can be caused to those least able to defend themselves against it. In order to ensure responsible use of the internet, all forms of social media and all online communications Conference workers will follow protocols and guidelines.

- In all communications workers should use language that is age-appropriate, clear and respectful.
- In relation to their own social media pages and contacts that they may have made through working for the Conference, workers will not invite or accept personal invitations to connect online with friends under 18 who are not family members. If it is deemed necessary to have a minor as a friend then the written permission of the parent of the minor is to be obtained outlining the necessary reasons for it.
- Workers will not use a pseudonym online.
- Workers must not use of the image of a child unless they have the written permission of the parent(s) or guardian(s) of the child.
- Workers must not post pictures of themselves alone with minors. An exception to this may be clearly formal group photos where the group being photographed are all minors such as a lunch of an event (Catholic Youth Festival).
- Workers must never send or receive images of a child or request from a child images of a child or children. If images of a particular child or children are received from a child, they should be deleted immediately and notify their supervisor.

9. Work Purposes and Other Use

The Conference provides its ICT resources for Conference work-related purposes and users must use them in accordance with this document and the other Conference policies. The Conference takes the act of logging on to its networks, websites and social media as an agreement to comply with the conditions for its use.

The Conference permits users to use its ICT resources for personal reasons only if such use is reasonable and kept to a minimum, does not interfere with Conference functions or with the user's duties and responsibilities to the Conference. Such use is subject to the requirements outlined in these guidelines and Conference's Use of Information Technology Systems Policy.

Large data downloads or transmissions should be minimised to ensure the performance of Conference ICT resources for other users is not adversely affected.

10. Illegal and Prohibited Use

Users must not use the Conference's ICT resources in any manner that is contrary to the law or likely to contravene the law. Electronic communications are subject to the full range of laws, including the laws of harassment, defamation, discrimination, privacy and copyright, as outlined below.

Harassment

Users must not use the Conference's ICT resources to send, publish or distribute messages that are harassing, obscene or threatening, nor may messages contain discriminatory, offensive or disruptive content. This includes sexually oriented messages and material or images and sexually harassing messages.

Users should be aware of and comply with the Conference's Antidiscrimination policy.

Defamation

Users must not use the Conference's ICT resources to send or publish material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or Conference liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

Discrimination

The content, style and tone of all messages and references to persons should avoid any comments or remarks that any reasonable person could interpret as distasteful or discriminatory. Messages that deal with political or religious beliefs, or with material that could be perceived as offensive or provocative based on sex, race, age, religion, national origin, disability, physical appearance or sexual orientation are not to be transmitted, downloaded or stored.

Gambling

The Conference strictly prohibits any form of gambling, other than those sanctioned by the Agency Head, such as a football tipping competition.

Confidentiality and privacy

Conference workers must not disclose personal or confidential information to which they have access unless required by the Conference or State/Territory or Commonwealth law to do so. In such cases, disclosure must comply with relevant privacy guidelines. All users should be aware that there is significant potential for breaches of privacy and security when using electronic communications.

As email is not a secure means of communication, emails are not private. Whilst the Conference makes every attempt to ensure the security of its network, users must be aware that the Conference cannot guarantee this security. Users must exercise caution in the disclosure of personal information through emails. Conference workers who in the course of their work have access to email and attachments concerning other people must take precautions to avoid invading individuals' privacy without their knowledge.

Where email involves the use of sensitive addresses, the Conference recommends that users make use of the Bcc field in their email program.

Any statement made by staff members, whether made online, offline or through images, videos or sound files, related to or referencing the Conference or any of its agencies, regardless of the media or forum used, must comply with this and other Conference policies and procedures.

Any internet-based conversation about the Conference and its agencies or the Catholic Church, Catholic religion or Catholic ethos should focus on publicly-known information. If a worker is not sure whether something is appropriate to post, they should consult their supervisor before posting.

Users should be aware of and comply with the requirements of the Conference's Privacy Policy.

Copyright infringement

When downloading or copying any material, users need to pay attention to the copyright conditions specified on the material.

Users must not distribute copyrighted material through email without specific authorisation to do so. Distributing copyrighted material by email increases the risk of copyright infringement and may give rise to personal and/or Conference liability, despite the belief that the use of such material was permitted.

The Conference will refer any suspected offender to the police or other relevant authority and the Conference may terminate their employment.

In relation to email, the Conference does not permit the following:

- Use of Conference and Conference agency contacts on Microsoft Outlook for personal use or gain
- Use of non-Conference accounts (such as BigPond, Hotmail) for Conference business
- Use of another worker's email address without approval

If in doubt about particular usage of Conference's ICT resources in relation to copyright, users should seek advice from their supervisor and/or their ICT function.

11. Access and Monitoring

Electronic communications created, sent or received using Conference's ICT resources are the property of the Conference and **an** authorised **person** may **access** the material in the case of an investigation, including in relation to investigations following a suspected breach of the IT Use Policy or procedures. Electronic communications may also be subject to discovery in litigation and criminal investigations.

The Conference will carry out any monitoring or surveillance of ICT use according to applicable State/Territory law.

Filtering software used by the Conference blocks most sites deemed inappropriate. The Conference can produce a breach report identifying any blocked site and the name of the person attempting to access the site. Authorised personnel check this breach report on a regular basis.

12. Security

1. The Conference requests users to be mindful of the potential for viruses and security breaches occurring because of sending or opening improper email communications and accessing electronic material on the internet. While virus protection software is in place, observance of reasonable precautions is critical. These may include deleting email received from unknown senders, attachments without messages, or email with generic subjects or attachments.
2. Malware has the potential to damage seriously Conference's ICT resources. Do not open any attachments or click on any links embedded in an email unless you have confidence in the identity of the sender.
3. Electronic and web communications are potential delivery systems for computer malware. Users must take care to download only materials from reputable websites.
4. Users are accountable for all use of ICT resources that the Conference has made available to them for work purposes and all use of Conference ICT resources performed with their user-ID. Users must maintain full supervision and physical control of Conference's ICT resources, including notebook computers, smart phones and tablets, thumb drives and external hard drives at all times. Users must keep User-IDs and passwords secure and confidential. Users must not allow or facilitate unauthorised access to Conference's ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.
5. Smart phones and tablets must be password protected.
6. For privacy and security reasons users must not leave confidential information on computer screens when workstations are unattended.
7. Hackers may modify communications to reflect a false message, sender or recipient. In these instances, an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, the user should take action to verify their identity by other means. A user should inform his or her supervisor if he or she believes that a hacker has intercepted or modified an electronic communication.
8. Active sessions are to be terminated when access is no longer required and computers secured by password when not in use.
9. If users detect problems related to the security of Conference's ICT resources, an immediate referral to your supervisor, Agency Head or the ICT Function in your agency is essential.

13. Records Management

Workers using email must ensure that they continue to maintain official records of the Conference. Users must file or forward to the records officer or archivist a copy of any message that relates to the business of the Conference. If unsure of whether you need to archive an email, consult the Records Manager or Archivist function.

Users are responsible for the content and maintenance of their own electronic mailboxes.

Retention of email messages fills up large amounts of storage on the network and can slow down performance. As few messages as possible should be maintained in a user's mailbox. Users should

keep messages for archive in separate archive files stored on the user's network home or shared drive.

14. Complaints

If Conference workers wish to make a complaint because they believe they have been subject to an inappropriate use of the Conference's ICT network, they should raise it with their supervisor. If their supervisor is the subject of their complaint, they should raise it using the Conference's Grievance procedure ([HR-PRO-011](#)).

15. Breaches

Breaches to these guidelines will result in disciplinary action, which may result in the termination of employment.

Any user who becomes aware of misuse of the Conference network has a responsibility to report it to their Supervisor, Agency Head or ICT Function in their agency.

Users who breach these guidelines may:

- Be required to attend appropriate counselling or interviews, and/or
- Have access to email and internet removed, and/or
- Subject him/herself or others to legal liability

Agency Heads will contact users who appear on a breach report attempting to access inappropriate sites, send offensive or inappropriate material, or breach these guidelines in other ways, for an explanation.

Wilful access to blocked sites, (especially where these sites are pornographic), or repeated breaches of these guidelines, may lead to disciplinary action including the termination of employment.

16. Records

Induction Checklist ([HR014](#))

Records of ICT use

Records of emails