OFFICE OF THE BISHOP

03.01 G
Information and Communication Technology Guidelines

INTRODUCTION

The Lutheran church of Australia (LCA) has prepared guidelines to assist committees, congregations, parishes and agencies to achieve the objectives of the LCA's Information and Communications Technology Policy, namely that

- ICT resources are used effectively across the LCA
- an integrated and reliable ICT platform is in place to meet the needs of the LCA
- the LCA's intellectual property and physical resources and assets are protected
- a safe environment is in place for users of ICT in accordance with scriptural principles and legal obligations.

Guidelines have been prepared covering the following areas

1. Digitally Stored Data
2. Electronic Messaging
3. Social Media
4. Internet
5. Discussion Lists and Blogs
6. Hardware
7. Software
8. People Skills
9. Threat Management

LCA agencies[1] are encouraged to adopt these guidelines as their procedures for use of ICT, or to develop their own procedures to cover their specific needs.

It is intended that these guidelines will be reviewed and updated regularly. The LCA ICT Advisory Committee (email: ictcommittee@lca.org.au) invites comments and suggestions.

[1] Defined in the LCA Governance Framework as follows: 'A board, commission, committee, council,department or tribunal of the Church; a board, committee, council or department of a district of the Church; and a member congregation or parish of the Church'

1. DIGITALLY STORED DATA

Wherever practical only one copy of each file/document should be stored.

Information should be accessible to those who have a need and right to it.
People and job functions should have individual authentication (e.g. username and password) to access the data they need and should not share this authentication.

Processes should be in place to securely archive all data records.

2. ELECTRONIC MESSAGING

Access to electronic communications is a privilege, not a right. Users are responsible for their behaviour and communications. Users are expected to use the resources for the purposes for which they are made available and take due care and accept personal responsibility for reporting any misuse. Serious breaches of these guidelines will result in disciplinary action, including the possibility of termination of employment or dismissal from ministry.

Users must be aware that electronic communications sent and received using the agency's resources are not private. The agency reserves the right to inspect, download, release and archive messages and logs at any time without notice for appropriate purpose.

The following explanations apply to the content of all forms of electronic messages.

- **Inappropriate material:** Users must not send or distribute electronic messages containing inappropriate material, such as offensive jokes (text or graphic). This includes, but is not limited to, sound files, movie files or any form of such material.
- **Profanity or pornography:** Users must not send or distribute electronic messages containing profanity or pornography. The LCA Child Protection Policy, LCA Safe Place system, LEA Valuing Safe Communities Policy and Equal Employment Opportunity legislation apply to electronic content. Sending profane or pornographic material (of any degree) by any electronic means is an extremely serious matter .
- **Derogatory or inflammatory information:** Users must not send or distribute electronic messages containing derogatory, inflammatory, insulting or libellous information about any LCA agency, any other user, church member, associate or any other person whatsoever. Sending such information is a serious matter and will result in disciplinary action, and risks the possibility of legal action for defamation by an aggrieved person.
- **Impersonation or misrepresentation:** Impersonating or misrepresenting someone else in any manner is prohibited. This could include sending a message using someone else's identity or changing the text of a forwarded email in a manner that could change the original intention or tone.
- **Privacy and confidentiality:** Electronic communication is not guaranteed to be private and confidential and therefore due care should be taken.
- **Cyber Bullying:** Cyber bullying is a form of harassment and will not be tolerated. Refer to the LCA Prevention of Harassment & Abuse Policy.
- **Disclosing information:** Information must not be disclosed to the media or other third party without the authorisation of the approving officer within the relevant agency or, in the case of personal communication, the individual concerned.

- **Viruses:** Intentionally transmitting computer viruses or harmful software internally or externally is not permitted.

- **Criminal behaviour:** The LCA has a zero tolerance for criminal activity and any such alleged behaviour must be referred to the police.

If the content of a received message contravenes any of the explanations above, the matter should immediately be brought to the attention of the person's line manager or responsible officer.

Emails

- Management of emails must comply with relevant legislation (State and Federal Freedom of Information and Privacy Acts), internal policies and standards.

- All emails sent or received on behalf of an LCA agency form part of the agency's records and are, and always shall be, the property of that agency. Processes should be in place to securely archive all email records created or received by the agency. A management process to access archived material should be in place.

- Users are responsible for security of their password and should take all reasonable safeguards to protect it. A password should not to be shared with another person. Users should be held accountable for any misuse recorded under their account details if reasonable care was not demonstrated. If a user has reason to believe that their password has been compromised then the password should be changed immediately.

- Using email for personal purposes is not be permitted unless agreed with the person's line manager or responsible officer.

- Scanned written signatures pasted into electronic mail messages or other documents should not be used. Only a properly produced 'digital signature' should be used.

- Users must not respond to and/or encourage spam mail. Spam email should be deleted and reported in accordance with internal procedures.

Email Attachments

It is recommended that broadcast documents attached to emails should be in pdf format where possible. This will ensure that they cannot be easily modified, the file size is generally smaller and they are more likely to be readable by recipients.

Disclaimers

Disclaimers should be included in each email sent from, or on behalf of, an agency. Agencies should adopt a common practice for email disclaimer notices.

Following is a suggested notice:

> The information contained in this email, and any attachments to it, are for the use of the intended recipient and are confidential. If you are not the intended recipient, you must not use, commercialise, disclose, read, forward, copy or retain any of the information. If you have received this email in error, please delete it and notify the sender by return email or telephone on ..... The LCA does not warrant that any attachments are free from viruses or any other defects. You assume all liability for any loss, damage, or other consequences, which may arise from opening or using the attachments. Unless otherwise expressly stated by an authorised representative of the LCA any views, opinions and other information expressed in this message and any attachments are solely those of the sender and do not constitute formal views or opinions of the LCA.

3. SOCIAL MEDIA

Agencies should use social media where it supports their mission and ministry strategies, and their communication strategy reflects why and how it is to be used. Agencies should be aware of not only the benefits of social media but also the cost of human resources required to keep it operating effectively, as well as the potential damage it can cause if it is not utilised with due care.

Users must be trained in the use of social media so that they use it in a responsible and appropriate manner and do not expose the LCA and the agency to liability, litigation or adverse publicity. LCA policies, specifically the LCA Standards of Ethical Behaviour and the LCA Child Protection policies, should be adhered to at all times.

Unless prior approval has been given by the user's line manager or the responsible officer, users should not use social media for private purposes while using agency-owned computers and/or during working hours.

Personal profiles

Pastors, lay workers, employees and volunteers are encouraged to use suitable privacy settings to protect themselves. Personal social media pages of pastors, lay workers, employees and volunteers which can be viewed publicly must not contain inappropriate material, profanity or pornography, derogatory or inflammatory information or impersonate/misrepresent someone else.

Please ensure that you use your personal email address (not your LCA email address) for your social media access.

Group Profiles

Where an agency sets up a social media group for an event, ministry etc., there should be a specific written procedure covering use of the group.

The procedure needs to cover

- description of procedures, roles and how the social media supports the agency's communication strategy
- boundaries for appropriate and inappropriate use
- items which should not be posted
- restrictions (if any) on posting images, identifying people in captions or tagging people in images, without their consent (or the consent of their parent/guardian if they are under 18 years of age)
- restrictions on photos, phone numbers, addresses, birthdates, licence plates, information that indicates a person's identity, status or location
- acceptable social networking etiquette
- consequences of not following the procedure.

4. INTERNET USE

Internet access is provided for users to assist them to carry out their normal work-related duties. The use of the internet on LCA-owned computers is for work purposes only, unless agreed otherwise by the relevant line manager or responsible officer. Accessing or downloading material for private purposes is prohibited, unless prior approval by the line manager or responsible officer has been given.

The agency's responsible officer must be aware of all programs loaded on users' computing devices so that licensing and threat management software can be kept up to date. If a program is downloaded without the responsible officer's knowledge, it presents protection and legal risks.

Due care must be taken when downloading programs and data. Risks include:

- they may come with extra little programs or viruses - some of which send out information from the computing device. This presents the potential for a serious breach of confidentiality policy;
- the download can affect critical programs and software which can lead to reinstallation or reconfiguring of the computing devices;
- it can slow the computing device or network performance.

In developing an internet presence

- Congregations and agencies should ensure that they have a presence in Google and Apple Maps. Information on setting this up can be found by entering 'Google Places for Business' and 'How To Add Your Business Listing To Apple Maps' into a search engine.

- The agency's web manager or responsible officer should regularly check that no inappropriate material, including profanity, pornography, derogatory or inflammatory information has been added to the website by hackers or other unauthorised persons.

- Advise the LCA Web Manager (email: webmanager@lca.org.au) of the address of the website so that a link can be set up from the LCA website (www.lca.org.au) to the internet presence of the agency.

- LCA agencies with a separate Internet presence should display the LCA logo, identify themselves as an agency of the LCA, and display a link to the LCA homepage (www.lca.org.au).

- Information and resources should be stored once only on the internet, with links to access it from other internet sites, wherever this is practical.

5. LCA DISCUSSION LISTS AND BLOGS

LCA discussion lists and blogs (defined as those endorsed by the LCA and advertised through official media of the LCA) will be moderated. Moderators will not be identified. If the description and guidelines for a list or blog permit it, moderators will authorise broad and even controversial expression of opinion which does not necessarily reflect the views of the LCA. All discussion lists and blogs, however, are subject to the Terms and Conditions for the List or Blog which shall be approved by LCA Communications Coordinator (email: linda.macqueen@lca.org.au). Moderators are not required to provide reasons for disallowing posts, apart from referring to the relevant section of the Terms and Conditions.

6. ICT HARDWARE

ICT Hardware must be fit for purpose and should be registered in the agency's Asset Register

Plans should be in place to upgrade, replace, repurpose or dispose of hardware which is no longer required or fit for purpose. Prior to the time of disposal of ICT hardware, any stored data/configuration must be securely erased.
At the time of discovery of loss of ICT hardware, the function of the device should be rendered inoperable.

Wherever practical, hardware devices should be networked.

The LCA ICT Advisory Committee (email: ictcommittee@lca.org.au) can provide advice/recommendations with respect to the adoption and purchase of ICT hardware which serves and supports the work of the LCA and its agencies.

7. ICT SOFTWARE

Software will be used which meets the operational needs of the LCA Agency. The software needs should be evaluated on a regular basis. The number of licenses needs to reflect the licensing terms of the software and the needs of the organisation.

A register should be maintained of software licences.

The LCA ICT Advisory Committee can provide advice/recommendations with respect to the adoption and purchase of ICT software which serves and supports the work of the LCA and its agencies

8. ICT PEOPLE SKILLS

Users should have suitable skills and be competent in the use of the available resources.

Where appropriate, training in the proficient use of the resources supplied must be made available.

9. ICT THREAT MANAGEMENT

Physical Security

Users must take due care with the physical security of hardware they are using.

Backups

All corporate data must be regularly backed up and backups stored in a secure manner and location, with at least one current backup stored off site. Backup and disaster recovery plans and processes will be in place. An appropriate number of copies (usually two) of backups will be made to different storage media. Regular checks will be made to ensure that backups can be restored. The business process cycle should be considered when determining the frequency of backups so that data can be restored without loss of significant information.

Electronic Security

A firewall should be enabled on each device and configured for appropriate security.

Wi-Fi networks should be secured in a manner appropriate to the situation.

Up-to-date threat management software (including, but not limited to, antivirus software) should be installed on all relevant computing devices.

Regular monitoring (checks) should be made for critical/security updates for applications, operating systems and other software and these will be deployed in a structured way.

Directories/folders and access permissions should be set up in such a way that people can share files on a needs basis, according to their authorised level of access.

Authentication

All computing devices which give access to corporate data should be protected from unauthorised access.

The strength of authentication (including passwords/biometrics) should be appropriate for the data being accessed.

Passwords should be changed on a regular basis.

Screensaver protection, with a password lock, should be set on computing devices.

All access rights should be revoked at cessation of pastors, lay workers, employees' or volunteers' requirements for access.

Document Controls

Document ID:	03.01 G
Prepared by:	ICT Advisory Committee
Approved by:	EOC
Document ownership:	OOB
Approved publication:	9 February 2016
Review date:	9 February 2018