Lutheran Church of Australia

2010.09 Information and Communication Technology Policy

2010.09 Policy

Background

This policy recognises the role and responsibility of the Lutheran Church of Australia (LCA) to both 'tend the flock' (1 Peter 5:1) and to be Christ's witnesses to those outside our church (1 Thess 2:10; Col 4:5). It supports the building up of Christian community (Ephesians 4:15,16) and the sharing of God's word with everyone (2 Tim 4:2). This policy helps the LCA to communicate God's love through Jesus Christ and be a place where love comes to life.

Information and communication technology will be used to contribute to and support this vision by facilitating communication and engagement, the sharing of information and the provision of resources. This policy outlines how this can be done in a manner consistent with our calling to be a place where love comes to life.

Objectives

The objectives of the ICT policy are to ensure that:

- all parts of the LCA are using ICT to improve their efficiency and effectiveness and ensure that best use is made of available resources;
- appropriate security protocols are put in place to protect the resources and the projects to which the resources are directed;
- all parts of the LCA can communicate and work together efficiently and effectively;
- the LCA uses ICT to effectively outreach to the community;
- ICT enables the LCA to use new initiatives and act as a catalyst for improvements in culture and work practices;
- LCA information is reliable, current and available.

These objectives will be achieved when:

1. **Digitally Stored Data** is treated, managed and controlled as a valuable asset;
2. **Electronic Messaging** is used in a manner appropriate to its nature as a rapid and efficient means of communication which may contain information of a confidential or sensitive nature;
3. **Social Media** is used appropriately, effectively and responsibly;
4. **The Internet** is used appropriately, effectively and responsibly;
5. **ICT Hardware** which allows applications to be used efficiently;
6. **ICT Software** is appropriate for operational requirements;
7. **ICT People Skills** are in place;
8. **ICT Threat Management** is in place to protect against threats including, but not limited to, viruses, malware, spyware, software or hardware failure, theft, fraud and unauthorised access;
9. **Legislation is** adhered to.

Policy Statement

All agencies of the LCA (as defined in Appendix 1) are required to implement a policy covering each of the areas outlined above. These policies will apply to all LCA representatives of the agency and need to be supported by procedures that will ensure responsible use and adherence to the available resources and set appropriate boundaries for users to follow.

Agencies will be required to comply with the general objectives outlined in this policy statement and use the guidelines in Appendix 2 as appropriate to their operation. The aim of the policy is that an agency's policies will eventually meet the requirements of this document as a minimum. Under the terms of the implementation guidelines it is understood that this may take some time.

The policy does not apply to students, clients, residents or patients of agencies covered by the policy.

Breaches of this policy will be managed through the relevant agency's internal performance management process and may lead to disciplinary action against the user.

Policy Framework

The activities listed below are by no means exhaustive due to the changing nature of the internet and electronic media however they attempt to provide a framework for following agreed policy guidelines in a responsible manner.

1. **Digitally Stored Data**

   Digitally stored data will meet relevant Australian Federal & State and New Zealand legislative requirements and internal policies including the LCA Professional Standard Unit's Privacy & Confidentiality Policy.

   Processes will be in place to securely archive all data records of the organisation.

2. **Electronic Messaging**

   All users are responsible for their behaviour and communications. All users are expected to use the church's resources for the purposes for which they are made available and take due care and accept personal responsibility for reporting any misuse.

3. **Social Media**

   Agencies of the church are encouraged to use social media where this fits their overall mission and ministry strategies. Like most good tools they are effective when used in a responsible manner but can cause damage when applied without due care. Agencies of the church are encouraged to use common sense and care when using this evolving medium. It is important that LCA representatives do not expose the LCA and the agency to liability, litigation or adverse publicity due to their social network behaviour.

   LCA representatives are expected to use social media in a responsible and appropriate manner. The LCA's ChildSafe and Safe Place policies in particular, as well as other relevant church policies, should be adhered to at all times.

4. **Internet Use**

   Internet access is provided for LCA representatives to assist them to carry out their normal work-related duties. The use of the internet is for work purposes only unless agreed otherwise by the relevant line manager.

   Downloading programs or data from the internet is prohibited unless prior approval by the line manager has been given.

5. **ICT Hardware**

   ICT Hardware must be fit for purpose and the agency should have procedures that include asset registers, maintenance and replacement of equipment.

6. **ICT Software**

   Software will be used which meets the operational needs of the LCA agency and the agency should have procedures that cover compliance with licensing and access.

7. **ICT People Skills**

   LCA representatives need to have appropriate skills and be competent in the use ICT resources.

8. **ICT Threat Management**

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

   Backup and disaster recovery plans and processes will be in place.

   Appropriate security of electronic data should be in place.

   All devices which give access to church data must be protected from unauthorised access.

9. **Legislation**

   All agencies must comply with legislation for their jurisdiction.

Responsibility for Reviewing and Updating the Policy

The LCA Information & Communications Technology Committee will review and update this policy, at least every two years, for approval by the General Church Council.

Responsibility for Compliance with the Policy

The LCA Business Manager is responsible for ensuring that all LCA departments, boards, councils and committees are aware of this policy

LCA district administrators are responsible for ensuring that all district departments, boards, councils, committees and congregations are aware of this policy.

Boards, councils and committees of the LCA and districts are responsible for the implementation of this policy and ensuring ongoing compliance.

Document Controls

Document ID:	2010:09 V1
Prepared By:	John Zeppel, Richard Frahm, Rodney Schwarz
Reviewed by:	LCA ICT Committee
Policy Ownership:	General Church Council
Draft publication:	Feb-13
Comments made by	Feb-13

Appendix 1 – Definitions

- **Agencies**: includes, but not limited to,
  - LCA National office
  - LCA District offices
  - Aged care facilities,
  - Bookshops,
  - Camps & conference centres,
  - Community care services,
  - Parishes congregations and worship centres
  - Schools, kindergartens & pre-schools
  - LCA boards, commissions, committees, tribunals, councils and auxiliaries,
  - LCA District boards, commissions, committees, tribunals, councils and auxiliaries, ,
  - Australian Lutheran College

- **Church**: Lutheran Church of Australia
- **Computing devices:** includes desktop and lap top computers and other mobile devices (eg i-phones, blackberries, android phones, tablet computers, etc)
- **Electronic messaging**: includes telephone, email, SMS and MMS messages, blogs, Facebook, Twitter, and other similar social network messaging.
- **ICT:** Information and Communication Technology
- **LCA Connect**: the LCA communications and engagement department
- **LCA representatives**: includes all pastors, lay workers, employees and volunteers.
- **Line Manager:** the person to whom the ICT user reports
- **Social Media:** includes web-based and mobile based technologies which are used to turn communication into interactive dialogue between organisations, communities, and individuals and covers, but is not limited to Facebook, Twitter, MySpace, Tumblr etc

Appendix 2 - Policy Guidelines

This section gives details of the types of statements and procedures that could be included in agency or site specific policies. They are included to assist with developing policy and procedure that is appropriate to the operation of the agency. The list is not exhaustive.

1 Digitally Stored Data

Wherever practical there will be one copy only of information stored - copies of the same or similar data will not be stored in different databases, spread sheets, documents etc.

Information should be accessible to those who have a need and right to it subject to limitations highlighted above.

People and job functions will have individual authentication (eg username and password) to access the data they need and must not share this authentication.

2 Electronic Messaging

Access to electronic communications is a privilege, not a right. All users are responsible for their behaviour and communications. All 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.

All users must be aware that the electronic communications sent and received using the agency's resources is 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. LCA Child Safe Policy, LCA Safe Place Policy, LEA Valuing Safe Communities policies and Equal Employment Opportunity laws apply to email content. Sending pornographic material (of any degree) by email is an extremely serious matter and may lead to termination of employment.
- *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.
- *Altering forwarded information:* Users must not alter forwarded information.
- *Impersonating or misrepresenting someone else via electronic messaging:* Impersonating or misrepresenting someone else in any manner, including via email, for example a user sending a message using someone else's identity, is strictly prohibited.
- *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 Professional Standard Unit's Anti-bullying & Harassment Policy.
- *Disclosing information:* Information will not be disclosed to the media without the authorisation of the relevant Church agency or the individual concerned.

- *Viruses:* Intentionally transmitting computer viruses or harmful software internally or externally is not permitted
- *Criminal behaviour:* Involvement in criminal behaviour is not acceptable.

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. The organisational escalation and/or complaints procedure will then apply.

Emails

Management of emails must comply with relevant legislation, internal policies and standards (eg. the Freedom of Information and Privacy Act 1988).

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

Users are responsible for security of their password and must take all reasonable safeguards to protect it. A password must not to be shared with another person. Users will 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 must be changed immediately.

Using email for personal purposes is not permitted unless agreed with the person's line manager.

Use of scanned written signatures pasted into electronic mail messages or other documents is not permitted. Only a properly produced "digital signature" should be used. Users must not respond to and/or encourage spam mail. All spam email should be deleted and reported in accordance with internal procedures.

Email Attachments

It is recommended that broadcast final 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 more recipients.

Notices on Emails

Notices (Disclaimers) will be included in each email sent from, or on behalf of, the office of a LCA agency.

Agencies of the LCA will have an agreed practice on the use of notices on emails. LCA representatives will be informed of the use of any applicable organisational notice.

Following is a recommended notice:

> *"This email, including any attachments, is confidential. If you have received this email in error, please advise the sender and delete it and all copies of it from your system. If you are not the intended recipient of this email, you must not use, print, distribute, copy or disclose its content to anyone.*
> *Although this email and its attachments are intended to be virus or defect-free, it is your responsibility to check for viruses and defects before opening and/or sending them on."*

LCA Email Addresses

LCA email addresses (eg '…@lca.org.au') have been implemented by the LCA to:

- improve the efficiency of communication by email within the church;

- facilitate the use of email as the preferred means of non-verbal communication in the LCA;
- identify the person or organisation as part of the LCA;
- provide easy to use, standardised, and intuitive email addresses for people who need to contact pastors, lay church workers and congregations;
- provide a permanent email address which will not change (to the outside world), even if pastors, lay church workers or congregations change their Internet Service Provider (ISP) or their local email address. This means that there is no need to notify others when changing a personal email address;
- simplify the administration associated with keeping up to date the email addresses of pastors, lay church workers and congregations in various directories, address books, databases, websites and documents.

LCA email addresses will be allocated to the following people and agencies where they are contactable by email:

- people on the LCA Roll of Pastors (including emeriti);
- people on the LCA Roll of Lay Workers;
- Australian Lutheran College pastoral students who have been approved for vicarage;
- LCA National Office employees;
- LCA District office employees;
- LCA congregations and worship centres (preaching places);
- LCA boards, councils, committees and commissions;
- LCA national and district auxiliaries.

LCA email addresses will be used in the LCA Yearbook, on the LCA website and in LCA publications and databases.

LCA email addresses will follow the following formats:

- **pastors, lay workers, LCA National Office staff and volunteers as agreed by the LCA directors** - preferedname.surname@lca.org.au (eg martin.luther@lca.org.au);
- **district office employees and volunteers as agreed by the district president** - preferredname.surname@district.lca.org.au (eg kate.luther@nsw.lca.org.au);
- **congregations and worship centres** - [name.]place.state@lca.org.au. Examples of congregation email addresses are stjohns.perth.wa@lca.org.au, and bethania.qld@lca.org.au;
- **LCA and district groups etc** - group[.state]@lca.org.au – state would be shown for state-based groups but would not be shown for national groups. (eg the email address for the LCA's ICT Committee is ictcommittee@lca.org.au).

LCA Email 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 Coordinator LCA Connect. Moderators are not required to provide reasons for disallowing posts, apart from referring to the relevant section of the Terms and Conditions.

Refer Appendix 3: Terms & Conditions sample (to be added)

LCA Domain Names

The LCA owns and manages the domain name "lca.org.au". The LCA IT Officer (itofficer@lca.org.au), will set up, at no cost, subdomains of lca.org.au for congregations/parishes and other LCA agencies and groups. Subdomains (preferably short and including a name or abbreviation which has an obvious connection to the agency or group) can be set up for either web or mail hosting or both.

3 Social Media

Personal profiles:

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

Group Profiles

Where an agency sets up a social media group for an event, ministry etc, there will 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

The use of the internet on LCA owned computers is for work purposes only unless agreed otherwise by the relevant line manager. Internet sites that may be seen as offensive must not be accessed using computing devices.

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;
- the site responsible officer must be aware of all programs loaded on individual computing devices so that licensing and threat management software can be kept up to date. If a program is downloaded without knowledge it presents protection and legal risks.

Websites

The **LCA's website** (www.lca.org.au) is the church's information hub, providing overviews of the LCA's mission and ministry, news, resources, and stories about the LCA and its people. It is designed to not only inform but also engage and inspire.

Districts of the LCA have individual website (www.state.lca.org.au) to meet their own specific requirements.

LCA Agencies: are encouraged to publish information and resources on the internet. Where they do not have their own internet presence, it can be provided to the Coordinator LCA Connect for review and placing on the LCA website.

Congregations and parishes are encouraged to develop their own internet presence with information specific to ministry in their area.

LCA Agencies with ministries to specific groups are encouraged to develop their own internet presence to promote and provide information about their agency.

In developing an internet presence

- inappropriate material, including profanity, pornography, derogatory or inflammatory information must not be included;
- links will be set up from the LCA website (www.lca.org.au) to the internet presence of all agencies of the LCA;
- LCA agencies with a separate internet presence will display the LCA logo, identify themselves as an agency of the LCA, and display a link to the LCA homepage;
- information and resources will be stored once only on the internet, with links to access it from other internet sites, wherever this is practical.

5 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 will be securely erased.

At the time of discovery of loss of ICT hardware, the function of the device will be rendered inoperable.

Wherever practical, hardware devices should be networked.

6 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.

7 ICT People Skills

Users must 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.

8 ICT Threat Management

Physical Security

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

Backups

All corporate data will 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 must be enabled on each device and configured for appropriate security.

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

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

Regular monitoring (checks) must 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 LCA representatives can share files on a needs basis, according to their authorised level of access.

Authentication

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

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

Passwords must be changed on a regular basis.

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

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

9 Legislation

All agencies must obey legislation for their jurisdiction. This includes, but is not limited to copyright, privacy, licensing, work place health and safety, child protection, harassment, equal opportunities, and commercial legislation.

Appendix 3: Terms & Conditions

To be added

Appendix 4: Policy Checklist

The following checklist has been prepared to assist agencies to review their compliance with the LCA ICT Policy. It is intended to be used in conjunction with the policy.

1 Digitally Stored Data

- ☐ Meets Legislative requirements
- ☐ Meets LCA privacy and confidentiality policies
- ☐ Archive process in place
- ☐ Authentication in place

2 Electronic Messaging

- ☐ Meets policy requirements

3 Social Media

- ☐ Meets policy requirements
- ☐ Meets LCA ChildSafe policy
- ☐ Meets LCA Safe Place policy
- ☐ Written procedure in place for each agency social media group

4 Internet Use

- ☐ Meets policy requirements
- ☐ Use of Internet is as agreed

5 ICT Hardware

- ☐ ICT hardware fit for purpose
- ☐ Asset register maintained
- ☐ Maintenance plan maintained
- ☐ Replacement plan maintained

6 ICT Software

- ☐ Fit for purpose
- ☐ Software register maintained
- ☐ Software licenced correctly

7 ICT People Skills

- ☐ People have appropriate skills and competency

8 ICT Threat Management

- ☐ Physical access to hardware is managed
- ☐ Backup and restore processes defined
- ☐ Backup and restore processes verified
- ☐ Electronic data security plan and authentication in place
- ☐ Threat management (including anti-virus) software up-to-date

9 Legislation

- ☐ Complies with relevant legislative requirements.