CATHOLIC ARCHDIOCESE OF SYDNEY

Acceptable Use Policy

Updated as at 15 March 2021.

1 Purpose of this Policy

The Catholic Archdiocese of Sydney (**Archdiocese**) provides employees (and other users) with access to an electronic mail system, which includes email, internet facilities and other computer systems and resources including laptop computers and mobile devices (together these systems and resources are collectively referred to as the **ICT Systems**). The ICT Systems are provided as tools of trade and for business purposes to enable both the employee (and other users) and the Archdiocese to perform efficiently with respect to the organisation.

2 Who does this Policy apply to?

This Policy applies to:

- all employees of the Archdiocese;
- all employees working at Domus Australia in Rome, Italy;
- bishops, priests, and seminarians (**Clergy**) and members of religious orders (**Religious**), who use the ICT Systems;
- volunteers;
- temporary staff; and
- private consultants, contractors, agents and clients of the Archdiocese

  (collectively, **users**).

Audit and other compliance measures will be instigated from time to time to ensure that the Policy is being complied with. All users need to be aware that monitoring and auditing will detail sites visited and downloads from a user’s computer, and may review the contents of users’ emails to assess compliance with this Policy.

3 Access to the ICT Systems

(a) <u>Access requirements</u>

A user is not permitted to access the ICT Systems without:

- reading and understanding this Policy; and
- authorisation from the Archdiocese, as evidenced by the allocation of an individual user id and password.

A user is not permitted to access the ICT Systems from a computer or device which does not comply with the ICT Standard Operating Environment guidelines for Device and Endpoint Security (as detailed in **Annexure B**).

(b) Business purpose

The ICT Systems are deployed for the Archdiocese. The ICT Systems are provided to users to facilitate communication and access to information for the Archdiocese's business purposes.

(c) Prohibited use

Users must not use the ICT Systems to:

- contravene the ethos and values of the Catholic Church;
- intentionally disseminate malware, viruses, adware, or software designed to exploit system resources;
- make illegal copies of any electronic files including software, music, movies or any other commercial electronic material;
- copy or use software in a manner which is inconsistent with a supplier's licence;
- download or upload unreasonably large amounts of media content (such as videos, photos, software, or music) unless it is for a business purpose;
- vilify, discriminate or harass another person or for the purpose of other unlawful activity; and
- access material that is profane or obscene (including pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people. This includes using social network sites to access or post such material.

(d) Prior written approval for any software or system

Users must not install, subscribe to, or utilise any software or system (including online services) without prior written authority from the ICT Manager.

Users must not enter into an agreement or make payments to any software provider without prior written authority from the ICT Manager and the General Counsel.

(e) Breach of software licences

The Archdiocese must comply with the software licensing requirements of their suppliers. Any breach of software licensing can attract significant penalties including potential legal action. Software licences are subject to regular audits by suppliers or their agents.

No user is permitted to install unlicensed software on the ICT Systems.

(f) Maintaining security

Users must take reasonable steps to protect the ICT Systems from unauthorised access.

(i) Password & Account Security

All users are required to comply with the Account Security Policy set out in **Annexure A**.

Users must take reasonable measures to keep their password secure, and should not disclose their password.

(ii) Security over computer and mobile devices

Lost or stolen computer or mobile devices must be reported immediately to the ICT Manager so that appropriate action can be taken to secure the device and any information contained within the device.

(g) Reporting security issues

If users become aware or suspect that the ICT Systems have been accessed by an unauthorised party (i.e. breached or hacked into), or that personal or confidential information has been lost or disclosed to an unauthorised party, they must immediately follow the steps set out in the **Data Breach Response Flowchart for Agency Heads and Agency Staff** (available on the CAS Agency Intranet at **link**).

For employees working at Domus Australia, please follow the steps set out in the **Data Breach Response Flowchart for Domus Australia**.

Additionally, if a password (or other system access control mechanism) is suspected of being lost, stolen or disclosed to an unauthorised party, the user must notify the ICT Manager immediately.

(h) Security training

From time to time, the ICT team conducts mandatory security training programs and seminars. Users are expected to attend and participate in these training programs, and seek guidance if they have concerns or uncertainty about their content and requirements.

(i) Electronic document retention

Wherever practicable, business and work-related documents must be saved onto iManage or Chancery/Agency-specific network folders. The practice of saving documents onto iManage and Chancery or Agency-specific network folders:

(i) ensures that documents are routinely backed up and retained;

(ii) ensures that a user has authorised access to particular documents; and

(iii) conforms with disaster recovery protocols.

4 Use of the Archdiocese email system

(a) Business purpose

The Archdiocese email system are provided to users for business purposes. However, it is recognised that users may, on limited occasions, send or receive communications by email for their personal use. The level of private use must be reasonable. A common sense approach will prevail. Such privileges will be withdrawn if they are abused.

(b) Prohibited Use

Users may not use the Archdiocese email system:

- to disclose confidential information pertaining to the Archdiocese;
- to forward any electronic documents to private web-based email accounts for non-work related purposes;
- from any personally owned mobile device, or using a mobile app, unless the user has reviewed and agreed to the Archdiocese Mobile Device Policy;
- to generate or forward to other people material that is inconsistent with the teachings of the Catholic Church or would otherwise discredit or in any way damage the reputation or image of or harm the Catholic Church;
- to generate personal profit or gamble;
- to send or forward chain letters or engage in “spamming”. (“Spamming” is sending an annoying or unnecessary message to a large number of people);
- in a way that may be considered illegal, offensive, defamatory, obscene, pornographic, discriminatory, harassing, victimizing, bullying, insulting or disruptive to another person. This would include accessing, viewing, downloading, printing or sending communications or attachments which contain:
  - language that is not appropriate in the workplace (for example, profanity or sexually explicit references);
  - sexually explicit communications or pictures;
  - offensive or inappropriate cartoons or jokes;
  - unwelcome propositions;
  - personal comments about colleagues;
  - ethnic or racial slurs;
- to access another person’s email account unless authorised by that person to do so;
- to register for online shopping portals or personal mailing list services (e.g. Amazon, Catch of the Day, Groupon) unless it is for business purposes;
- to register for social media accounts (e.g Facebook, Twitter, Instagram, YouTube) unless it is for business purposes;
- to distribute personal information about a person without that person’s consent; and
- to download or distribute copyright material of third parties without the copyright owner’s consent, including software, database files, documentation, pictures, articles, graphic files, text or other information, or to otherwise infringe intellectual property rights.

Users should be aware that engaging in prohibited activities will be treated as a disciplinary matter and may have consequences for your employment. If the activity is illegal, the matter will be referred to the police for action.

(c) Security protections

Users are expected to conduct their email-related activities in a manner that promotes and preserves the security of the ICT Systems.

Users must not attempt to circumvent the Archdiocese's security systems (such as its email filtering system, which guards against spam and malicious emails). Users are expected to maintain a reasonable level of diligence in identifying and reporting spam or malicious emails.

Users are required to participate in regular mandatory email security testing and training. The Archdiocese may use cyber-security test emails to assess and develop the level of awareness and preparedness of users to defend against email-based cyberattacks.

5 Use of the Archdiocese Internet system

(a) Business purpose

The Archdiocese Internet system is provided to users for business purposes. However, it is recognised that users may, on limited occasions, access the Internet for their personal use. The level of personal use must not be significant and must not interfere with a user's work obligations.

(b) Prohibited use

Users must not use the Archdiocese Internet system (including social media sites) to:

- contravene the ethos and values of the Catholic Church;
- to generate or forward to other people material that is inconsistent with the teachings of the Catholic Church or would otherwise discredit or in any way damage the reputation of or harm the Catholic Church;
- access, view, download, print, disseminate or post any material that may be considered inappropriate, offensive, defamatory, obscene, pornographic or discriminatory including material that is sexually explicit or that has racist, sexist, or political content or which includes inappropriate comments in relation to sexual orientation, disabilities or any other physical attributes;
- download any software from the Internet unless it is for business purposes;
- download or upload unreasonably large amounts of music, photographs, video clips, games, screen savers, wallpaper files or other multimedia content (unless it is for a business purpose);
- use pirate software sites and similar activities;

- post any information on internet news groups, bulletin boards or similar forums on behalf of the Archdiocese unless expressly authorised to do so by the Executive Director, Administration and Finance or the Director of Communications; or
- misrepresent or attempt to misrepresent the identity of the computer user.

6 Audit procedures

All email messages and internet access logs are the Archdiocese's records. The Archdiocese reserves the right, consistent with previous versions of this Policy, to:

- continuously monitor and record, through the use of software, email messages and Internet access by users (which may include personal information about users);
- access email accounts at any time and from time to time and without prior notice to the user;
- disclose the contents of business email messages within the Archdiocese without a user's permission;
- disclose the contents of personal email messages and internet logs within the Archdiocese without a user's permission to enable the Archdiocese to ascertain whether there have been any breaches of the law or this Policy; and
- disclose the contents of personal email messages and Internet logs to third parties without a user's permission to enable the Archdiocese to take appropriate action in relation to any breach of the law or this Policy.

This Policy may be updated from time-to-time.

Annexure A: Account Security Policy

1 Purpose

The purpose of this annexure is to provide guidance on the specific requirements for account security, which applies to all users of the ICT Systems. It includes steps which may be taken to further secure sensitive or 'administrator' accounts.

2 Account security

The ICT team recognises that account security as a concept has changed significantly in the past five years, to include many factors beyond simple password strength.

Sensitive accounts

Sensitive accounts are:

- accounts that hold particularly sensitive or confidential information; or
- accounts of users who have access to, and interaction with, systems containing sensitive or confidential information.

For example, sensitive accounts include accounts of senior managers, users with access to payroll functions, accounts of legal staff, safeguarding office staff, employment services staff, and assistants to senior managers. These accounts are subject to higher levels of scrutiny and may require additional security measures (depending of the level of sensitivity of the information) such as:

- lockdown of account access, requiring a user to be within the office to access systems;
- enforcement of higher password strength requirements;
- enforcement of multi-factor authentication steps; or
- additional logging and scrutiny of account activity.

Administrator accounts

Accounts with administrator access to any systems are subject to higher security requirements, which may include the following:

- where possible, the administrator account must be separated entirely from the user's regular account. The administrator account must only be used when conducting operations requiring that level of privilege;
- enforcement of higher password strength requirements;
- where possible, multiple-factor authentication is implemented and is used by the user; and
- additional logging and scrutiny of account activity is carried out.

Review and classification of accounts

The ICT team will regularly review and update a complete list of accounts which fall within sensitive or administrator accounts for the purpose of auditing of security controls and access.

3 Passwords

The schedule below sets out the minimum standard applicable to all users. A more stringent requirement may be enforced on sensitive accounts, administrator accounts, or other identified accounts or groups of accounts.

Expiry time	180 days
Is expiry time enforced?	Yes
Remembered passwords	10
Minimum password length (in characters)	15
Account lockout	Yes
Login attempts before account lockout	10
Lockout duration	15 minutes
Password complexity requirements	A password must contain all of the 4 following attributes: • Uppercase Letter (A- Z) • Lowercase Letter (a – z) • Numeral (0 – 9) • Special Character (!@#$%^&*()_+)

4 Other guidelines when using passwords

- Never store passwords in an unsecured location, or within the account itself.
- Never use your work password for personal external accounts (such as Facebook or Gmail).
- You can also see if your email account or password may have been disclosed in a data breach via the website at https://haveibeenpwned.com/.

Annexure B: Device & Endpoint Security

1 Purpose

The purpose of this annexure is to detail the specific security and reliability requirements and configuration expected of computers, mobile devices, and other endpoints (collectively, **Devices**), where used by users, to access the ICT Systems.

2 Standard Operating Environment

The ICT team constantly maintains and updates a 'Standard Operating Environment' (**SOE**) set of configurations which are applied to all Devices issued by the Archdiocese.

The SOE includes the following features necessary for system security and reliability:

- Sophos Endpoint Protection Antivirus and Security Management;
- Windows BitLocker Full-Drive encryption;
- Network Security Group Policy;
- Firewall Network Security Policy and Web Filtering; or
- other non-specific security products and features as required.

Users must not circumvent, disable, or tamper with the SOE under any circumstances.

In limited circumstances, the Archdiocese may issue Devices that do not confirm to the SOE. For example, legacy systems used to run old applications or bespoke devices used for a specific purpose.

Devices issued by the Archdiocese that do not conform to the SOE will not be granted access to the ICT Systems, unless prior written approval is granted by the ICT Manager.

The ICT team is not able to deploy SOE or any other software on a user's personal Device.

3 Access from a user's own personal Device

A user may access particular services (such as the Archdiocese's webmail service) within the ICT Systems using the user's own personal Device. For example, a user may access their work email via the user's personal mobile phone, or via citrix remote login on the user's personal computer.

When using a personal Device to access the ICT Systems, the user must take reasonable steps to verify that the Device:

- has a reasonably up-to-date operating system and software;
- has an up-to-date and functional antivirus program; and
  can be 'trusted' in the context of the intended access. e.g. users must not use a public terminal to login and view confidential or sensitive documents.