uniting church
in Australia,
Synod of NSW & ACT

# Information Protection

**Title:** Information Protection Policy
**Creation Date:** August 2021
**Version:** 0.1
**Last Revised:** March 2022
**Approved by:** Synod Office SLT

# Table of Contents

# 1. Overview/Background

In the course of our work in communities, the Uniting Church of Australia (‘**Church’**) and the Synod of NSW and ACT (‘**Synod’**) may collect or be in possession of personal or sensitive information.

At all times, we will honour the faith afforded to us by members of our congregations and communities by taking all reasonable steps to protect all personal or sensitive information in our possession. This means we carefully consider what information we collect, as well as how we store, retrieve and share information.

These principles relate equally to information we collect and hold on our employees, Ministers, volunteers and independent contracts and consultants.

# 2. Purpose of Policy

This policy sets out our information security protocols for information in either electronic or physical storage or use.

# 3. Applicability (scope)

This policy applies to all employees, Ministers, volunteers, independent contractors and consultants (‘**individuals’**).

All individuals have a responsibility to protect personal or sensitive information in their possession and to only use that information for the purpose for which it was gathered (‘**primary purpose’**). Definitions of personal and sensitive information can be found in the Definitions section of this policy.

# 4. Responsibilities

### 4.1 General Secretary, Senior Executives and Directors

- The General Secretary owns this policy and is accountable for ensuring the implementation of this policy across the Synod. The General Secretary has a legal and moral responsibility to protect confidential and sensitive information.
- The Senior Executives and Directors are responsible for;
  - The implementation and communication of this policy within their divisions and functional areas and for identifying any processes or procedures necessary within their divisions to ensure compliance with this policy; and
  - Ensuring any breaches, or potential breaches, of this policy are appropriately reported and that both corrective and preventative actions are identified and taken.

### 4.2 Policy Owner and Sponsor

- The Chief Operating Officer is responsible for implementing and overseeing this Policy and for ensuring Individuals are aware of their obligations under this policy.

### 4.3 People Managers

- People Managers are responsible for:

  - Ensuring appropriate protocols and procedures are followed to ensure protection of confidential and sensitive information;
  - Promptly reporting any breaches of this policy and taking action only after consultation with the Director People & Culture?/Compliance Team?
  - Maintaining confidentiality of any breaches or transgressions under this policy except insofar as is necessary to appropriately report or deal with any issues arising under this policy.

### 4.4 Individuals

- Individuals are responsible for:
  - Understanding and complying with this policy;

    Immediately reporting any actual or potential breaches of this policy to their People Manager;
  - Following protocols and procedures identified as part of this policy;
  - Remaining vigilant to any unauthorised attempts to obtain confidential or sensitive information.

## 5. Principles

Although as a non-profit organisation, the Church and the Synod are permitted to collect sensitive information without a person's express consent, we will always endeavour to seek consent as a matter of respect for those associated with us in whatever capacity.

The Synod will only collect information necessary to carry out our work and at all times we will operate in line with the National Privacy Principles and relevant state and territory legislation. In essence:

- We will only collect information necessary to carry out our work;
- We will not ask for personal or health information unless a primary purpose has been defined and outlined to the person(s) involved;
- We will not disclose personal or health information without the person's prior consent;
- Those whose information we hold have the right to access or change that information (the exception to this is employee files for either past or existing employees as these are exempt from the National Privacy Act);
- Where a person asks to see or change the personal or sensitive information we hold about them, the Synod reserves the right to charge a modest administration fee;
- De-identified information or information in the aggregate may be used or shared with other Church bodies or agencies in support of the Synod's work;
- All personal or sensitive information will be stored securely;
- Information security protocols (outlined in this policy) will be communicated to individuals together with expectation of individuals' behaviour when dealing with personal or sensitive information;
- We hold confidentiality and privacy dear, regardless of whether it relates to an individual or a Synod congregation or community member.

# 6. Collecting and storing confidential information

Personal and sensitive information may only be used for its primary purpose. Where information is to be used for a secondary purpose (i.e. something beyond the scope of the primary purpose), the Synod will seek the advance consent of the person in writing.

Information will be held securely in electronic version with necessary password protection applied to ensure access is restricted only to those who require it in the course of their work. Additionally, the Synod has set up a series of secured folders which can be shared within teams but not among teams (e.g. data and information held by People and Culture can only be seen, identified and accessed by those within the People and Culture team).

# 7. Protecting confidential information

The Synod has outlined a number of guidelines to be followed by individuals when handling or sharing confidential information and to protect our IT systems generally.

Individuals should only access confidential, private or sensitive information as relevant and necessary to their work.

### 7.1 Handling confidential information

When handling or sharing handling confidential information:

- confirm recipient details before sending and consider whether email is sufficiently secure to protect the information from unauthorised access;
- any sensitive, personal or proprietary information should be encrypted and attached to an email rather than laid out in the body of the email; ideally the document password will be shared via means other than email (e.g. SMS);
- hard copy information should always be stored in a locked filing cabinet or room. In this regard it is not appropriate to take hard copy information out of the office, or to print hard copy versions of documents in a home office unless it can be locked away;
- be aware of your surroundings and people nearby as they may be able to read documents or hear conversations;
- any unwanted hard copies of information are to be shredded or placed in one of the secure bins in the Synod's offices;
- avoid sharing any confidential information through internet-based file-sharing software (e.g. Dropbox).

### 7.2 Portable storage devices

Although small, portable storage devices can store large amounts of information. Examples of portable storage devices include:

- removable media (e.g. CD-ROMs, DVDs, USB drives);
- digital MP3 players (e.g. iPods);
- laptops, tablet computers and slates (e.g. iPads);
- smartphones (e.g. iPhones).

Using portable storage devices to access, store or transport personal information can involve considerable risk because:

- they can be easily lost or stolen, and then accessed by unauthorised people;
- using them in public can increase the chance of accidentally disclosing confidential information to others.

To minimise the information security risks associated with using portable storage devices, individuals should not use these devices for confidential information.

### 7.3 Unsolicited and suspicious emails

Unsolicited emails can contain viruses that threaten the security of information stored on users' computers. If you receive an email from an unknown sender or an unexpected email from a known sender and it looks suspicious, do not click on any links or attachments contained in the subject line or body.

Email scams are increasingly sophisticated often closely mimicking someone we know. Please take a few seconds to check the email address of the email before diving in and acting on the email. If you are uncertain, please speak with IT or your People Manager. Alternatively, you may wish to call the individual who purportedly sent you the email to check its legitimacy (or otherwise).

### 7.4 Clear desks and screens

Work environments should be clear of confidential information when unattended. This means:

- not leaving documents containing confidential information unattended on printers, photocopiers or desks;
- locking the computer screen when leaving it unattended;
- only printing documents when absolutely necessary;
- storing portable storage devices and hard copies of confidential information in a secure drawer or cabinet, not on your desk.

### 7.5 Information disposal

Ensure record retention requirements have been met prior to the disposal of any business information. When disposing of confidential information, either shred them or use the secured bins available at the Synod's offices.

Any confidential information stored on electronic media including computers, hard drives, and USB keys should be thoroughly cleaned and sanitised when the information is longer required.

### 7.6 Visitors

To help minimise the risks to the security of personal information:

- ensure all visitors are registered, their identity verified, and that they're accompanied at all times
- be alert to the practice of tailgating when entering the Synod's premises
- be aware of unaccompanied people who you do not recognise
- notify your manager if you believe an unauthorised person is present on the premises.

From time to time maintenance people will be on site to check and/or fix air conditioning, lighting or printers (to name a few). If unsure whether they're authorised, please share your concern with the operations team.

## 8. Privacy incidents

Privacy and information security incidents may happen frighteningly easily. Examples of incidents include:

- accidental download of a virus onto a Synod computer;
- clicking on phishing links[1];
- discussing or sharing of confidential information on a social networking website;
- loss or theft of a portable storage device including mobile devices containing personal information;
- non-secure disposal of hard copies of confidential information (i.e. placing readable paper in recycle bin or hard waste bin);
- unencrypted documents sent to the wrong email address.

Privacy and information security incidents can:

- occur due to accidental or deliberate actions
- result from human error or technical failures
- apply to information in any form, whether electronic or hard copy.

### Incident reporting

It is vital that any incidents are reported to IT or your People Manager as soon as possible so that the impact can be assessed and minimized. Where personal or sensitive information has been shared, the Synod may have an obligation to contact the persons whose information has been disclosed and to notify the Office of the Australian Information Commissioner.

## 9. Definitions

**'Biometric information'** is an electronic copy of a person's face, fingerprints, iris, palm, signature or voice.

**'Confidential information'** includes personal information, sensitive information and any Church or Synod proprietary information or information which is not, and is not intended to be, in the public domain.

**'Personal information'** includes a broad range of information, or opinion, that could identify a person. Personal information could include:

- A person's name, signature, address, phone number or date of birth;
- Sensitive information (see definition);
- Credit information (see information);
- Employee record information;
- Photographs;
- Internet protocol (IP) addresses;

[1] Phishing is a method of trying to gather personal information using deceptive e-mails and websites

- Voice print and facial recognition biometrics;
- Location information from a mobile device.

**'Sensitive information'** is personal information that includes information or opinion about a person's:

- Racial or ethnic origin;
- Political opinions or associations;
- Religious or philosophical beliefs;
- Trade union membership or associations;
- Sexual orientation or practices;
- Criminal record;
- Health or generic information;
- Some aspects of biometric information.

## 10. Breaches of this policy

Individuals found to be in breach of this policy could face disciplinary action up to and including termination of employment depending on the seriousness of the policy breach.

## 11. Policy review

This policy will be reviewed three years from its implementation or soon as required by legislative changes or circumstances.

## 12. Terms and Conditions

This Policy does not form part of any contract of employment or contract of engagement and may be amended, replaced or revoked at any time by the Synod at its discretion.