



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

1. PURPOSE

A policy for the Diocese on appropriate, efficient and effective use of Information Technology, including Cybersecurity best practices, as well as use of Artificial Intelligence (AI) systems.

2. SCOPE

This applies to all ministry units of the Diocese, with the exception of Anglicare North Coast, the Diocesan Schools, and the Lismore Parish Centre Preschool. It applies to all ministry unit (including the Registry) clergy, office holders, staff and volunteers.

3. INFORMATION TECHNOLOGY

3.1 Adequate Resourcing

Computers, printers, and other technologies are vital to the work of the Diocese. All Ministry Units are to ensure that they are adequately resourced to conduct their work. At a minimum, each parish office should have a computer, phone and printer to conduct parish business. Each Incumbent should also be issued with a laptop and mobile phone.

It is recognised that people working (including volunteers) may have different ability levels with technology, so Ministry Units are to provide training (whether formal or informal) as required to ensure efficient use of IT systems.

3.2 Appropriate Use

Ministry Unit IT resources are to be used appropriately. The business of the Ministry Unit is the primary purpose of assigned computers and phones, with limited personal business acceptable as long as it does not interfere with other duties.

All technology is to be used in alignment with the law, as well as any other Diocesan policies and guidelines, especially GEN-001 Privacy Policy, and GEN-008 Use of Social Media

Any form of unlawful, offensive or harassing use of IT resources is unacceptable. Faithfulness in Service and Diocesan policy around bullying and harassment apply in full to online and digital behaviour.

3.3 File Management

All Ministry Units hold electronic files and records for their day-to-day use. In order to ensure they are accessible, recoverable, and subject to appropriate governance, a file platform such as OneDrive or SharePoint should be used for file storage rather than local device storage.



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

Files of a sensitive or confidential nature (including financial records, personnel files or parishioner personal information) must be held in access-restricted folders, and be accessed only by people authorised to view them. Personally Identifiable Information (PII) must further be held in alignment with GEN-001 Privacy Policy.

4. CYBERSECURITY

4.1 Cybersecurity Standards

The Australian Cyber Security Centre has developed a set of eight baseline mitigation strategies, known as the Essential Eight, to help organisations protect themselves against common cyber threats. While designed primarily for larger organisations and government, the underlying principles are relevant to Ministry Units and must be applied, at a scale appropriate to their size and resources.

- Application control:** Restricting which software and applications are allowed to run on Ministry Unit computers, so unapproved or malicious programs cannot execute.
- Patch applications:** Regularly updating software (such as web browsers, PDF readers, and office applications) to fix known security weaknesses before they can be exploited.
- Configure Microsoft Office macro settings:** Blocking or restricting macros in Word, Excel, and other Office documents from the internet, since malicious macros are a common way attackers deliver malware.
- User application hardening:** Disabling unnecessary or risky features in web browsers and applications (such as ads) to reduce the ways an attacker can gain access.
- Restrict administrative privileges:** Limiting who has "administrator" access on computers and systems, so that if an account is compromised, the damage an attacker can do is minimised.
- Patch operating systems:** Keeping computer and device operating systems (such as Windows or iOS) up to date with security fixes.
- Multi-factor authentication (MFA):** Requiring a second form of verification (such as a code sent to a phone) in addition to a password, making it much harder for stolen passwords to be used.
- Regular backups:** Making regular backups of important data and testing that they can be restored, so information is not permanently lost in the event of a ransomware attack, hardware failure, or human error

4.2 Cybersecurity Incidents

There are many forms of Cybersecurity Incidents that a Ministry Unit may face. The below is a non-exhaustive list of potential cybersecurity threats that may be seen:

- Phishing emails**
Fraudulent emails designed to trick the recipient into clicking a link, opening an



ANGLICAN DIOCESE OF GRAFTON POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

attachment, or providing information such as passwords or bank details. These often impersonate a trusted person (a Rector, Bishop, Diocese officer, or supplier) and create a sense of urgency.

b) **Business email compromise**

A scammer impersonates a senior figure, usually by email, asking for an urgent payment, gift cards, or a change to banking details. These messages are often sent when the real person is known to be away or busy, making the request harder to verify quickly.

c) **Invoice or payment redirection fraud**

A criminal poses as a known supplier or contractor and asks for future payments to be sent to a new bank account. This is particularly relevant for Ministry Units managing building works, maintenance contracts, or regular supplier payments.

d) **Ransomware**

Malicious software that locks or encrypts files on a computer or network, with the attacker demanding payment to restore access. This can affect parish registers, financial records, or shared drives, and can spread through infected email attachments or compromised websites.

e) **Account takeover**

An attacker gains access to a Ministry Unit email account, social media page, or online banking login, often through a weak or reused password or a successful phishing attempt. Once inside, they may send fraudulent messages to parishioners or attempt to access financial systems.

f) **Data breaches**

Unauthorised access to, or accidental disclosure of, personal information such as parishioner names, addresses, financial details, or safeguarding records. This can happen through hacking, lost or stolen devices, or simple human error (e.g. an email sent to the wrong recipient with sensitive attachments).

g) **Malware and viruses**

Harmful software that can infect a computer through infected email attachments, malicious websites, or infected USB devices, potentially damaging files or allowing unauthorised access.

h) **Social media impersonation or hijacking**

An attacker creates a fake parish social media page or takes control of an existing one to solicit donations, spread misinformation, or scam parishioners and the wider community.

i) **Physical device theft or loss**

Laptops, tablets, or phones containing Ministry Unit data can be lost or stolen. Without proper safeguards (passwords, encryption, remote wipe capability), this can lead to a broader data breach.



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

4.3 Basic Security Management

Ministry Units must take basic security precautions to ensure the security and integrity of their IT systems and information.

Some measures Ministry Units can take include:

- Using strong, unique passwords for every account.
- To the extent possible, not sharing passwords.
- Not writing down passwords. If needed, a password manager should be used.
- Removing access and changing passwords to a generic email when a volunteer, staff member, or clergy person leaves their role.
- Not clicking links from unknown or unexpected senders, and checking the sender's actual email address to ensure it comes from the purported sender.
- Regularly update all Ministry Unit devices with security patches as suggested by the Operating System and IT service providers (if applicable).
- Maintain antivirus and security software on Ministry Unit devices.
- Confirm any change to bank details (e.g. a supplier or contractor asking to update payment details) via a separate, verified communication channel before acting on it.

4.4 Response and Recovery

Every Ministry Unit must have a Cybersecurity Response Procedure and Plan, which outlines how they will respond to an incident as described in 4.2. The Registry will develop a template procedure and plan for assisting Ministry Units in Cybersecurity response, coordinated by the Diocese's Chief Information and Digital Officer (CIDO).

At a minimum, a ministry unit shall inform their IT service provider (if applicable) within one hour of becoming aware of a Cybersecurity Incident, and the Chief Information and Digital Officer as soon as practicable after that. They are then to follow the advice of their IT provider or CIDO in managing the response.

5. ARTIFICIAL INTELLIGENCE

5.1 What is Artificial Intelligence?

Artificial Intelligence (AI) refers to technologies that can perform tasks that would normally require human thinking, including analysing data, producing content and supporting decision-making.

The most common form of AI Ministry Units will use is Generative AI, which is used to create



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

text, images, or audio based on user prompts.

5.2 Appropriate Use

Ministry Units may use AI tools to support their work where that use is lawful and consistent with this policy and other Diocesan policies, including GEN-001 Privacy Policy. AI is a tool to assist people. It does not replace the judgement, discernment or accountability of the clergy, staff and volunteers using it.

Tools

- Use AI tools provided or approved by the Ministry Unit. The Registry will keep a list of approved tools that a Ministry Unit may choose from.
- Free or public AI tools generally offer no protection for what is entered into them, and may store or reuse it. Check with the Registry before using a tool that has not been approved.
- AI features built into other software (such as email, video conferencing, design and transcription tools) are covered by this policy.

Suitable uses

- Drafting or editing newsletters, notices, rosters, social media posts and routine correspondence.
- Summarising publicly available documents.
- Brainstorming ideas for events, programs and study groups.
- Preparing first drafts of resources, which the responsible person must review and adapt.
- Improving the clarity, tone and accessibility of the user's own writing.

Information that must not be entered

- Personally Identifiable Information about parishioners, clergy, staff, volunteers or the public.
- Safeguarding records, complaints, and any information about children.
- Pastoral conversations and confidential information shared in ministry
- Personnel and recruitment information.
- Financial records, bank details, passwords and access credentials.
- Legal advice, contracts, and confidential papers of the Bishop-in-Council, Corporate Trustees or Synod.

Only the Registrar or Chief Information and Digital Officer can approve an exception, and only for an assessed tool. Safeguarding, pastoral and confessional information must never be entered into an AI tool.



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

Uses that are not appropriate

- Making, or being the sole basis for, decisions about people, including appointments, employment, discipline, safeguarding assessments and financial assistance.
- Replacing personal pastoral communication. Condolence letters and messages to people in distress must be written by the person sending them.
- Creating images, audio or video of real people, or content that impersonates a person, particularly clergy or children.
- Recording or transcribing meetings without telling participants and obtaining their consent. AI note-takers must not be used in confidential meetings.

If confidential information is entered into an AI tool in error, treat it as a Cybersecurity Incident under 4.2 and report it as set out in 4.4.

5.3 Attribution

The person who uses AI to help create content remains its author and is responsible for it. Ministry Units should be open about their use of AI where it matters to the reader.

When to disclose

- Disclose where AI has produced a substantial part of a report, submission, grant application or formal document provided to the Diocese, Bishop-in-Council, a funder, or a government body, or where the recipient requires it.
- Disclosure is not needed for minor assistance such as spelling, grammar or formatting.
- Suggested wording: *"This document was prepared with the assistance of [tool] and reviewed by [name]."*

Images and media

- Label AI-generated images in newsletters, websites and social media.
- Do not present AI-generated images as photographs of real events, people or places.

Quotes, sources and copyright

- Never attribute AI-generated words to a real person, including the Bishop, clergy or other public figures. Verify any quote against its original source before use.



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

- AI can reproduce copyrighted material without warning. Check text, images and music (including hymn and song lyrics) before publishing and confirm that the Ministry Unit's licences cover the use.
- Content generated by AI may not be protected by copyright in Australia, so it should not be treated as original work of the Ministry Unit without significant human authorship.

Ministry & Worship

- Those preparing sermons, prayers or liturgical material are responsible for their theological soundness and faithfulness to authorised texts, whether or not AI was used in preparation.

5.4 Errors and Hallucinations

Generative AI can produce content that reads confidently and is wrong. These errors are often called hallucinations. Examples include invented facts, references and web links, incorrect dates and figures, fabricated quotes or Bible verses, outdated information, and inaccurate statements of law. AI outputs may also reflect bias.

Human review

- All AI output must be read and checked by a person with enough knowledge of the subject before it is used, sent or published.
- Apply more scrutiny where an error could cause harm, including legal, financial, safeguarding, employment, WHS, property, contract and cemetery and burial matters.

Verification

- Check facts, figures, names and dates against a reliable primary source.
- Confirm that every reference, link and quote exists and says what the AI claims.
- Check Scripture, prayers and liturgical text against the authorised source, not the AI output.
- Be especially cautious with legislation, case names, and anything stated with unexplained certainty.

Professional advice

- AI is not a substitute for legal, financial, tax, insurance, engineering or other professional advice. Ministry Units should seek advice through the Registry or a qualified professional.



ANGLICAN DIOCESE OF GRAFTON

POLICIES AND PROCEDURES

SUBJECT: Information Technology, Cybersecurity and Artificial Intelligence Policy		PROCEDURE REFERENCE NUMBER GEN-017
DATE APPROVED 8 October 2026 by Bishop-in-Council		REVISION NUMBER Version 1
IMPLEMENTATION DATE Immediate	REVIEW DATE AND FREQUENCY 2 Yearly	RESPONSIBLE FOR REVIEW Bishop-in-Council

Accountability and correction

- The person who sends or publishes AI-assisted content is responsible for it. An error made by the tool is not a defence.
- If an error has been published or sent, correct it promptly and tell the Registry if it may cause harm or reputational damage.
- If an error involves personal information, treat it as a data breach under GEN-001 and Clause 4.4.

6. Links and Additional Resources

1. [Cyber.gov.au](https://www.cyber.gov.au) – Cybersecurity resources for business and organisations
2. [Cyber Health Check Tool](#) - Tool for organisations to assess the strength of their cybersecurity protocols.
3. [Report | Cyber.gov.au](#) – Portal for reporting Cybersecurity Incidents
4. [Essential Eight maturity model](#) – Information on the Essential Eight Model