Anglican Diocese of
BENDIGO

CYBER SECURITY POLICY

Version: 1.0	*Date of Issue:* August 2023
Contact: Registrar	*Review Date:* August 2024

Introduction

While the Anglican Diocese of Bendigo wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the organisation's systems are controlled, and the organisation is protected against the damaging actions of others.

Our policy aims to:

This policy sets out guidelines for generating, implementing, and maintaining practices that protect the organisation's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

Application:

This policy applies to employees, contractors, consultants, and volunteers at the Registry Office at the Anglican Diocese of Bendigo, including all personnel affiliated with third parties, to all equipment owned or leased by the Anglican Diocese of Bendigo, and to all equipment authorised by the Anglican Diocese of Bendigo for the conduct of the organisation's business.

Policy:

While the Anglican Diocese of Bendigo wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the organisation's systems remains the property of the Anglican Diocese of Bendigo. Because of the need to protect the Anglican Diocese of Bendigo's network, the confidentiality of information stored on any network device belonging to the Anglican Diocese of Bendigo cannot be guaranteed, and the Anglican Diocese of Bendigo reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Information in the possession of the organisation shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.

Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

Breach of this policy by any employee may result in disciplinary action, up to and including dismissal.

Responsibilities:

It is the responsibility of the Registrar to ensure that:

- staff are aware of this policy;
- any breaches of this policy are dealt with appropriately;
- a report on the organisation's cyber security is submitted annually to the Diocesan Executive and Bishop in Council;
- any changes to the organisation's cyber security requirements are addressed.

It is the responsibility of all employees and volunteers to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any particular instance, employees and volunteers should consult the Registrar.

Processes:

1. Monitoring

1.1 The Registrar may authorise the monitoring of the organisation's equipment, systems, and network traffic at any time for security and network maintenance purposes.

2. Key digital assets and data

2.1 The Registrar shall from time-to-time issue cyber security procedures appropriate to different levels of data sensitivity.

2.2 The Registrar will maintain a register of the Anglican Diocese of Bendigo's key digital assets and data. This should include the nature of the data, where it is stored, who has access to it, who is protecting it, how well it is protected, the reason for holding the data and lifecycle management of the data.

2.3 Key digital assets and data shall be classified according to sensitivity and risk. Systems controls and access will be determined according to the level of sensitivity of the data.

2.4 The Registrar is required to review and approve the classification of the data and determine the appropriate level of access and security that will best protect it.

3. Access control

3.1 Individuals shall only be permitted access to the organisation's information resources necessary for them to perform their duties as part of their role. Access control shall be exercised through username and password controls.

4. Computer security

4.1 All PCs, laptops and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

4.2 Users must keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned. Authorised users are responsible for the security of their passwords and accounts.

4.3 All access accounts should be secured with a strong password and must have multi-factor authentication enabled.

4.4 Users who forget their password must call the IT service provider to get a new password assigned to their account. The user must identify themselves to the IT service provider, or have the request made by the Registrar.

4.5 Users will not be allowed to log-on as system administrators. Only the IT service provider can log on as system administrator.

4.6 Employee logins and passwords will be deactivated as soon as possible if the employment of the organisation. The Registrar shall immediately and directly contact the IT service provider to report a change in employee status that requires terminating or modifying employee login access privileges.

4.7 All computers and devices used by the user that are connected to the Anglican Diocese of Bendigo's IT infrastructure, whether owned by the user or the Anglican Diocese of Bendigo, shall be continually executing virus-scanning software with a current virus database approved by the IT service provider.

4.8 Malware protection software must not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.

4.9 Automatic updating of the malware protection software and its data files must be enabled.

4.10 All email attachments must be scanned. All documents imported into the computer system must be scanned. Weekly scanning of all computers should be enabled.

4.11 A record of the antivirus and anti-malware software should be kept.

4.12 Desktop computers in areas of public access should be physically secured by cables and padlocks.

4.13 Where possible, sensitive data should not be removed from the organisation's premises without specific authorisation.

4.14 Where this is not feasible, data on laptops that may leave the organisation's premises should be protected by full disk encryption. Staff who need access to sensitive data offsite should use a device owned by the organisation.

4.15 Computers being deaccessioned (whether for sale, reuse, or disposal) shall not be released until all data has been securely deleted.

4.16 Users shall not download unauthorised software from the internet onto their PCs or workstations.

4.17 Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses, malware, or Trojan horse code.

4.18 Users who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should

report the situation to the IT service provider immediately. The user shall not turn off the computer or delete suspicious files.

4.19 Users must not themselves breach security or disrupt network communication on the organisation's systems or elsewhere. Security breaches include accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access unless these duties are within the scope of regular duties. "Disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.20 Users shall not attach unauthorised devices to their computers unless they have received specific authorisation from the Registrar or the IT service provider.

5. Optional

5.1 Only authorised devices may be used to access the Anglican Diocese of Bendigo's IT infrastructure. Authorised devices include PCs and workstations owned by the Anglican Diocese of Bendigo and compliant with the configuration guidelines. Authorised devices also include network infrastructure devices used for network management and monitoring.

5.2 Users shall not use devices that are not authorised, owned, or controlled by the Anglican Diocese of Bendigo. Any personal devices used for work purposes (eg. working from home) must first be set up by the IT service provider. Users shall not attach to the network any unauthorised storage devices; e.g., USBs, writable CDs.

Related Documents: Internal

- Key digital assets and data register
- Privacy Policy

Approved by Bishop in Council:

1 August 2023

Anglican Diocese of
BENDIGO

Policy History	
Policy created	August 2023
Policy reviewed	
Policy amended	