INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

CONTENTS

1 PURPOSE 1
2 SCOPE 1
3 POLICY STATEMENT 1
4 RESPONSIBILITIES 2
Compliance, monitoring and review 2
Reporting 2
Records management 2
5 DEFINITIONS 2
Terms and definitions 2
6 RELATED LEGISLATION AND DOCUMENTS 2
7 FEEDBACK 3
8 APPROVAL AND REVIEW DETAILS 3
9 APPENDICES 4-8

1 PURPOSE

To set out information and communications technology (ICT) protocols and standards for use within the Diocese of North West Australia and its ministry centres.

2 SCOPE

This policy applies to the following areas:

2.1 Acceptable Use of Technology: Guidelines for the use of computers, fax machines, telephones, internet, email, and voicemail and the consequences for misuse.

2.2 Security: Guidelines for passwords, levels of access to the network, virus protection, confidentiality, and the usage of data.

2.3 Disaster Recovery: Guidelines for data recovery in the event of a disaster, and data backup methods.

2.4 Technology Standards: Guidelines to determine the type of software, hardware, and systems will be purchased and used in the Diocese, including those that are prohibited**.**

2.5 Network Set up and Documentation: Guidelines regarding how the network is configured, how to add new employees to the network, permission levels for employees, and licensing of software.

2.6 IT Services: Guidelines to determine how technology needs and problems will be addressed, who in the organization is responsible for employee technical support, maintenance, installation, and long-term technology planning. If some or all of these services are outsourced, who manages the outsourcing and how the outsource is chosen.

3 POLICY STATEMENT

The Diocese is committed to the following protocols and standards to ensure data is secure and used appropriately.

Acceptable Use of Technology

Information and communications technology is to be used as appropriate for the purpose of the Diocese and its ministry centres. This includes the use of computers, mobile devices, telephones, internet, fax, and voicemail. Use of this technology for both work and private purposes must at all times be consistent with the Diocesan Code of Conduct. For example, the technology should not be used to view "restricted material" or to communicate in a way that could cause harm to others.

Data Security
Data security is to be maintained at an appropriately high level depending on the nature of the data as outlined in Appendix 1.

Disaster Recovery
The Diocese and its ministry centres will take appropriate steps to ensure backup data is safely stored and current so that in the event of a disaster, the operations of the Diocese or ministry centre is able to be continued with minimum delay. Refer to the Guidelines in Appendix 2.

Technology Standards
The Diocese is committed to appropriate Technology Standards. This includes not downloading copyright materials unless used according to the Copyright Policy. Refer to the Guidelines in Appendix 3.

Network Set up and Documentation
The setup of networks in the Diocese is documented and includes instructions regarding how the network is configured, how to add new employees to the network, permission levels for employees, and licensing of software. Refer to the Guidelines in Appendix 4.

IT Services
A record is kept of whom in the ministry centre is responsible for technical support, maintenance, installation, and long-term technology planning. If some or all of these services are outsourced, this record includes who manages the outsourcing and how the outsource is chosen. Guidelines to determine technology needs and how problems will be addressed are found in Appendix 5.

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 The Diocesan Council is responsible for compliance of this policy by workers in its ministry centres. The Diocesan Registrar, assisted by the Diocesan Financial Officer, will monitor and review policy compliance on behalf of the Council.

Reporting

4.2 No additional reporting is required.

Records management

4.3 The Registry maintains all records relevant to administering this policy using its recordkeeping system.

5 DEFINITIONS

5.1 Terms not defined in this document may be found in the Diocesan Glossary.

Terms and definitions

Disaster
A disaster is any event that causes problems with personnel, computers or the internet which results in current data being lost or unavailable. This could include computer failure, storm damage, long term electrical outage; or death, incapacity or unavailability of personnel.

6 RELATED LEGISLATION AND DOCUMENTS

Copyright Policy

Privacy Policy

Diocesan Code of Conduct, *Faithfulness in Service*

7 FEEDBACK

7.1 Church members may provide feedback about this document by emailing registrar@anglicandnwa.org.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Diocesan Council
Administrator	Diocesan Registrar
Next Review Date	27/02/2024

9 APPENDICES

1. Guidelines for Data Security
2. Guidelines for Disaster Recovery
3. Guidelines for Technology Standards
4. Guidelines for Diocesan Office Network Setup and Documentation
5. Guidelines for IT Services

Appendix 1

GUIDELINES FOR DATA SECURITY

1 PURPOSE

Data security is to be maintained at an appropriately high level depending on the nature of the data.

2 SCOPE

Guidelines for passwords, levels of access to the network, virus protection, confidentiality, and the usage of data.

3 GUIDELINES

3.1 Password Security:

Personal logins and passwords should not be shared with anyone except the network administrator, IT Coordinator or Registrar. This information should be kept in a secure place and kept up to date. For example, in a password protected software file, as a paper list kept in a fireproof safe preferably offsite. Ministry centre wardens are to provide to the Diocesan Registrar a regularly updated copy of all Centre computer passwords so that in the event of a change of staff, continuity may be maintained. This also applies in relation to disaster recovery.

3.2 Levels of access to networks

Access to networks and data should be restricted so that personnel have appropriate access to the information they need to carry out their function or ministry. In general, only the network administrator or Senior Minister or Registrar should have unlimited access.

3.3 Virus Protection

Up to date virus protection should be in place on all computers and if possible, on the incoming server. The virus database should be set to update at least daily and data should be scanned regularly.

3.4 Confidentiality

Data should be kept confidential. During staff induction, this should be stressed. The DNWA Privacy Policy applies to much of the data kept by the Diocese or ministry centres.

3.5 Data usage

Data should only be used as required for the activities and purpose of the Diocese or ministry centre

4 RELATED DOCUMENTS

- Copyright Policy
- Privacy Policy

Appendix 2

GUIDELINES FOR DISASTER RECOVERY

1 PURPOSE

The Diocese and its ministry centres will take appropriate steps to ensure backup data is safely stored and current so that in the event of a disaster, the operations of the ministry centre Is able to be continued with minimum delay.

2 SCOPE

Guidelines for data recovery in the event of a disaster, other considerations and data backup methods.

3 GUIDELINES

3.1 Data Backup

The network administrator should ensure that data is regularly backed up and that it is possible to restore the data. The frequency of backup is decided by the ministry centre but should be frequent enough so that if a disaster occurs, minimal data is lost.

3.2 Management of Backups

- If data is held in the "cloud" then the network administrator must ensure that copies of the data are made regularly to another cloud site or that the contract with the cloud provider ensures that backups of the data are made with sufficient regularity so that should a disaster occur, the operation of the ministry centre is minimally affected.
- If data is held in the ministry centre, the data should be backed up regularly to an external device such as an external hard drive or memory stick. The backup should be held in a secure location, preferably remote from the site.
- Ideally if data is held in the cloud then a separate backup should be held locally but at a remote site.

3.3 Data recovery

The network administrator should ensure that it is possible to restore lost data by testing the restoration of data from backups from time to time.

3.4 Death or Incapacity of Personnel

Should a staff member or worker die, become incapacitated, or suddenly leave, thought should be given to carrying on that persons' function. Passwords, email addresses, computer access and other contact information should be available to allow this. This information should be held securely in a safe or online vault so that continuity is possible. This should include volunteers such as ministry centre treasurers and ministry coordinators. Ministry centre wardens are to provide to the Diocesan Registrar a regularly updated copy of all Centre computer passwords so that in the event of a change of staff, continuity may be maintained.

3.5 Storm and Tempest

- Since large parts of the Diocese is subject to cyclones, there should be consideration given to carrying on the ministry in the event of storm damage to equipment, buildings and infrastructure.
- There should also be a plan in place to manage the effect of power outages and the loss of phone and internet connections.

4 DEFINITIONS

Disaster

A disaster is any event that causes problem with personnel, computers or the internet which results in current data being lost or unavailable. This could include computer failure, storm damage, long term electrical outage or death, incapacity or unavailability of personnel.

Appendix 3

GUIDELINES FOR TECHNOLOGY STANDARDS

1 PURPOSE

The Diocese is committed to appropriate Technology Standards. This includes not downloading copyright materials unless used according to the Copyright Policy.

2 SCOPE

This guideline covers the type of software, hardware, and systems that will be purchased and used in the Diocese, including those that are prohibited (for example, instant messenger or media download software or apps that are inconsistent with the Diocesan Code of Conduct).

3 GUIDELINES

3.1 Type of Software

- Appropriate licenced software is only to be used in a ministry centre.
- Any software that encourages breach of copyright is not to be used.

3.2 Hardware

Hardware purchases must be compatible with existing hardware and approved by the person at the ministry centre whose role it is to manage IT.

3.3 Downloading from the Internet

- Materials downloaded from the internet must not breach the Copyright Policy or the Diocesan Code of Conduct
- Media downloads must not breach the Copyright Policy

4 RELATED DOCUMENTS

- Copyright Policy
- Diocesan Code of Conduct, *Faithfulness in Service*

Appendix 4

GUIDELINES FOR DIOCESAN NETWORK SET UP AND DOCUMENTATION

1 PURPOSE

The setup of networks in the Diocese is documented and includes guidelines regarding how the network is configured, how to add new employees to the network, permission levels for employees, and licensing of software.

2 SCOPE

This guideline includes how the IT network is configured, how to add new employees to the network, permission levels for employees, and licensing of software.

3 GUIDELINES

3.1 Documentation

The setup of networks should be documented to include structure and responsibility. Administrator password/s (see Appendix 1) and similar essential information should be securely recorded, to ensure continuity of operation should a change of personnel occur.

3.2 New Employees or Workers

The process of providing access levels, usernames and passwords to new users should be documented.

3.3 Software Licensing

All software used on a ministry centre computer must be licenced.

Appendix 5

GUIDELINES FOR IT SERVICES

1 PURPOSE

To document who in the Diocesan Office or ministry centre is responsible for network administration, technical support, maintenance, installation, and long-term technology planning. In addition, if some or all of these services are outsourced, who manages the outsourcing and how the outsourced service provider is chosen.

2 SCOPE

This guideline includes how IT needs and problems will be addressed, who in the organization is responsible for employee technical support, maintenance, installation, and long-term technology planning. If some or all of these services are outsourced, it also includes these outsourcing arrangements.

3 GUIDELINES

3.1 IT Management responsibility

- The Registrar is responsible for all IT management, assisted by the Diocesan Financial Officer.
- The Financial Officer provides inhouse IT support for minor issues and ‘helpdesk’.

3.2 Planning for Infrastructure acquisitions and upgrades

- The Registrar or Minister-in-Charge is responsible for determining needs and ensuring purchases are within budget.
- The Financial Officer provides advice on all purchases, e.g. ensures that *ad hoc* purchases do not occur and that any purchase of equipment is compatible with the existing infrastructure.

3.3 Maintenance

- For the Diocesan Office and mission districts, the Finance Officer is responsible for maintenance according to the following schedule:
  - software upgrades and operating system updates;
  - installing new software;
  - network maintenance; and
  - WiFi.
- For other ministry centres, a nominated member of Parish Council or a specified employee is responsible for maintenance according to the following schedule:
  - software upgrades and operating system updates;
  - installing new software; and
  - network maintenance; and
  - WiFi.

3.4 Outsourcing

- The following services are outsourced at the Diocesan office:
  - Offsite backups
  - Advanced IT support
  - Network upgrades
  - Network security
- The outsourced service provider is contracted according to the following guidelines:
  - Existing relationship, proven “track record” or suitable references;
  - Clearly defined scope for contract of services;
  - Documentation of the services they provide on a job-by-job basis; and
  - Registrar to manage this contract.
- Cloud Data
  - must concur with the Privacy Policy;
  - must be backed up; and
  - there must be a guarantee of supply.