# Anglican Diocese of The Murray

| Regulation: | Privacy Policy | | |
|---|---|---|---|
| **Body adopting** | Diocesan Council | **Date of adoption or last review:** | 6 April 24 |
| **Related Documents:** | Model Parish Privacy Policy<br>Privacy Policy information statement<br>Data Breaches Reporting Form | **Review schedule:** | 5 Years |

## Introduction & Rationale

To encourage sensitivity and appropriate respect for individuals in the collection and use of information for Church purposes.

To provide formal guidelines for the Diocese and Parishes to ensure protection of people's privacy in accordance with the Australian National Privacy Principles.

To provide a process for reporting data breaches or suspected data breaches to the Registrar to enable compliance with Notifiable Data Breaches (NDB) obligations introduced by the Federal Government in February 2018.

### Scope

This policy applies to all areas of the Synod and to all its activities in supporting Anglican ministry within the Anglican Diocese of The Murray (including undertaking safer ministry checks). All employees, officeholders, volunteers, consultants, contractors, and agents of the Synod are required to comply with this Policy when collecting Personal Information on the Synod's behalf and when dealing with Personal Information in the Synod's possession. Failure to do so may constitute grounds for disciplinary action.

This Policy does not apply to Anglican parishes, congregations or other worshipping communities located within the Anglican Diocese of The Murray however individual Parish Councils are required to adopt the Model Parish Privacy Policy and report any known or suspected data breaches to the Registrar.

### Policy Responsibility

The Diocesan Council is responsible for oversight of implementation and review of this policy.

The Registrar is responsible for managing and reporting any notifiable data breaches within the Diocese in accordance with statutory obligations and making recommendations to mitigate risks.

## Part A) PRIVACY PROTECTION GUIDELINES:

### 1. Collection

It is usual for the Diocese to collect personal information about Church members and potential Church members including their religious practices. In addition, it is usual for the Diocese and Parish Councils to collect information from service providers, contractors and agents. It is important that the collection of personal information is fair, lawful and not intrusive. A person must be told the name of our organisation, the purpose of collection and how to get access to their personal information and what happens if the person chooses not to give the information.

## 2. Use and disclosure.

In relation to Church Members or potential Church members it would be usual to collect from such individual, the individual's name, contact details, date of birth and history of Church membership.

In relation to individuals acting as service providers, contractors or agents of the Diocese it would be usual to collect from such individual the individual's name, contact details and relevant information concerning that individual's dealings with the Diocese.

Information should only be disclosed for the purpose it was collected (primary purpose) unless the person concerned has consented, or a secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure. A normal secondary purpose is communication about our activities, funding needs and philosophies.

## 3. Data quality

Reasonable steps must be taken to ensure that the personal information collected, used or disclosed is accurate, complete and up-to-date.

## 4. Data security

Reasonable steps should be taken to protect the personal information held from misuse, loss and from unauthorised access, modification or disclosure.

## 5. Openness

A Privacy Policy information statement should be available outlining the information handling practices of the Diocese and Parish Councils and made available to anyone who asks for it.

## 6. Access and correction

An individual has the right to access the personal information held by the Diocese about them. Unless exempted from doing so by law, individuals should be permitted access to their own records. It is intended that any request for such access be made through the Office of the Diocesan Registrar.

## 7. Identifiers

Identifiers that have been assigned by a Commonwealth Government agency (e.g. Tax File Number, Medicare number, Pension number etc.) should not be obtained, used or disclosed except where required by law (e.g. in the case of a Contractor – ABN No. or where funds are invested with the Diocese – TFN No.).

## 8. Anonymity

Individuals should be given the option to interact with the Diocese or a Parish Council anonymously whenever it is lawful and practicable to do so.

## 9. Transborder data flows

The Diocese should only transfer personal information to a recipient in a foreign country in circumstances where the information will have the appropriate protection.

## 10. Sensitive information

Sensitive information will not be collected unless a person has consented to its collection, it is required by law, or the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any other individual.

## Part B) DATA BREACH PROCEDURE:

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. The records may be stored electronically, or paper based. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and have the potential to cause harm to individuals and the church.

Some examples of a data breach include but are not limited to the following:

- where a device such as a mobile phone containing personal information of Parish members is lost or stolen
- where a database containing personal information is hacked
- a Parish makes personal information accessible or visible to others outside the organisation without permission.
- an email containing personal or sensitive information is sent to an external party in error.
- unauthorised access to personal information by a church worker or independent contractor.

If any church worker is aware of a data breach or suspects a data breach, they should notify the Registrar as soon as practical. Prompt action is generally the key to reducing the risk of harm. Once notified, the Registry team will work with the Parish to assess risks and act.

A data breach report template is provided on the Diocesan website under the Parish Tools section or the Diocesan Registry.

The template is designed to assist in gathering all relevant information that is known at that time. It may also assist to identify what immediate remedial action the Parish can take to reduce the risk of potential harm to individuals.

==========

**Acknowledgement**: *This policy has been adapted from the Privacy Policies of the Dioceses of Adelaide and Bendigo. We thank them for their work in this area and their willingness to share it.*

### Related Documents: External

**https://www.oaic.gov.au/privacy/privacy-act/national-privacy-principles**