DIOCESE OF LISMORE

Privacy (Internal) Policy

EFFECTIVE DATE	1 July 2020
REVIEW DATE	1 July 2023
POLICY OWNER	Chancery
APPLIES TO	This Policy applies to clergy, employees, contractors, volunteers, work experience students and trainees (**Workers**) of the Diocese.
EXCLUSIONS	Where an agency or entity of the Diocese has its own policy, the relevant agency or entity policy will apply to Workers engaged by those agencies or entities. In the event of conflict between the policies of agencies or entities and the Diocesan policy, the Diocesan policy prevails.
RELATED POLICIES, GUIDELINES & PROCEDURES	Privacy (External) Policy Acceptable Use of Electronic Communication Systems & Devices Policy Code of Conduct
REFERENCE	*Privacy Act 1988 (Clth)* *Privacy Regulation 2013 (Clth)*
RELATED FORMS	Office of the Australian Privacy Information Commissioner (OAIC) - Notifiable Data Breach Form
HEADINGS	Objective Definitions Policy 1. How the Diocese Collects Personal Information? 2. What is the difference between Personal Information and Sensitive Information? 3. Australian Privacy Principals 4. What Information does the Diocese Hold? 5. Purpose of Collecting Privacy Information 6. Consent 7. Website Usage and Privacy Collection 8. Storage of Information 9. Disclosure of Information 10. Accessing Stored Information 11. Accuracy of Information 12. Consequences of Not Providing Consent 13. Notifiable Data Breaches 13.1 Examples of Notifiable Data Breaches 13.2 Notification of Eligible Data Breaches 13.3 Initial Process for Suspected Data Breaches

OBJECTIVE

This policy ensures that Workers engaged by the Trustees of the Roman Catholic Church for the Diocese of Lismore gather, store, disseminate and dispose of Personal Information in such a way as to ensure that:

- the collection, use, storage, disclosure and dissemination of Personal Information occurs in accordance with the law;
- individuals who provide the Diocese with their Personal Information can be assured that it will be treated in a manner consistant with the law; and
- comply with the Notifiable Data Breaches (NDB) Scheme.

DEFINITIONS

Diocese means the Roman Catholic Diocese of Lismore and includes without limitation any Diocesan agencies, corporations, entities, parishes, parish corporations and parish entities where the Worker is employed or otherwise engaged.

Data Breach means an unauthorised access or disclosure of personal information, or loss of personal information.

Eligible Data Breach means a data breach where the following criteria is met:

- there is an unauthorised access to, or disclosure of personal information held by the Diocese (or information is lost in circumstances where the unauthorised access or disclosure is likely to occur); and
- this is likely to result in serious harm to any of the individuals to whom the information relates; and
- the Diocese has been unable to prevent the likely risk of serious harm with remedial action.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not.

Related Body Corporate means a body corporate that is a holding company of another body corporate, a subsidiary of the other body corporate, or a subsidiary of the holding company of that body corporate.

Response Team Coordinator means the Privacy Officer.

Secondary Purpose means any purpose other than the primary purpose for which the Diocese collected the personal information.

Sensitive Information means:

a) information or an opinion about an individual's:
    i. racial or ethnic origin; or
    ii. political opinion; or
    iii. membership of a political association; or
    iv. religious beliefs or affiliations; or
    v. philosophical beliefs; or
    vi. membership of a professional or trade association; or
    vii. membership of a trade union; or
    viii. sexual orientation or practices; or
    ix. criminal record;

    that is also personal information; or

b) health information about an individual; or
c) genetic information about an individual; or
d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
e) biometric templates.

Worker means clergy, religious, employees, board members, contractors, volunteers, work experience students and trainees of the Diocese.

POLICY

1. How the Diocese Collects Personal Information?

The Diocese, as part of the Roman Catholic Church, conducts a range of activities to fulfil its mission. Those activities include parishes, schools, healthcare facilities and welfare agencies as well as charitable works, and conducting activities that require the collection of Personal Information. Personal Information is also collected to enable the Diocese to minister to the faithful and to fulfil its canonical and civil obligations under the Code of Canon Law, government legislation and common law.

2. What is the difference between Personal Information and Sensitive Information?

Sensitive Information is Personal Information that is subject to a much higher level of privacy protection than other Personal Information. It can only be collected with consent, except in specific circumstances. Sensitive Information:

- must not be disclosed for a Secondary Purpose unless the Secondary Purpose is directly related to the primary purpose of collection and within the reasonable expectation of the individual to whom the Personal Information relates;
- cannot be shared by Related Body Corporates in the same way that Related Body Corporates may share Personal Information; and
- cannot be used for the Secondary Purpose of direct marketing.

3. Australian Privacy Principles

The Diocese is bound by the *Privacy Act 1988 (Clth)* (**the Act**). The Act contains thirteen Australian Privacy Principles (**APPs**), which outline how the Diocese must handle, use and manage Personal Information.

4. What Information does the Diocese Hold?

The Personal or Sensitive information that the Diocese holds about an individual may include, but is not limited, to the following:

- personal contact details;
- sacramental records;
- information relating to an application for employment;
- information about an individual that enables the Diocese to satisfy its duty of care to other individuals with whom a volunteer or employee may come into contact in the course of their involvement with the Diocese such as a criminal record or Working With Children Check;
- information relating to pastoral care needs;
- information relating to a child's enrolment at a Diocesan school;
- information relating to the provision of health or welfare services; and
- any other information about an individual that may be relevant to the contact that the individual might have with the Diocese.

5. Purpose of Collecting Privacy Information

The Diocese collects Personal Information for many purposes, including but not limited to:

- information needed to minister to the faithful and to provide pastoral care;
- information about an individual's educational needs and expectations in Diocesan schools;
- information about an individual's welfare and support needs;
- information to support or promote fundraising activities;
- information needed to administer sacraments;
- information about an individual's employment history or pre-employment screening to assess the employment applications of a prospective employee;
- information about bank accounts that might allow the Diocese to pay an individual; and
- information needed to keep parishioners informed about matters related to the Diocese, Parishes, Agencies and ministries through correspondence, newsletters and magazines.

6. Consent

The Diocese endeavours to collect Personal Information directly from the individual or their parent or guardian in the case of a child. Where this is not possible, consent will be sought prior to collecting the Personal Information from a third party. If consent cannot be obtained, the Diocese will have regard to the requirements and exemptions of the Act before deciding whether to collect Personal Information indirectly.

In the case of children, Personal Information will ordinarily be collected from their parents or guardians, unless specific and/or unusual circumstances require that the collection be made directly from the relevant child.

For prospective Workers, the Diocese may collect Personal Information by speaking with referees. The Diocese may contact applicants' previous employers who have not been nominated as referees. Should this be the case, applicants will be advised prior to such contact being made.

In some limited circumstances, contractors who have confidentiality agreements in place with the Diocese may have access to Personal Information stored by the Diocese.

7. Website Usage and Privacy Collection

The **Diocesan Privacy Policy** (**Privacy Policy**) is available on the Diocesan website (**the Website**). By using the Website, individuals agree to be bound by this **Privacy Policy**. Whenever an individual submits Personal Information to the Diocese, they consent to:

- the collection, use, disclosure and storage of that information in accordance with this **Privacy Policy**; and
- the receipt of emails or other communications about the Diocese and our activities (including information about marketing, promotional, and research purposes), along with communications about Catholic Church-related activities, functions, issues and initiatives from time-to-time.

8. Storage of Information

The Diocese takes reasonable steps to protect and secure Personal Information from unauthorised access, loss, misuse, disclosure or alteration. These steps include restricted access to Diocesan offices and other areas where Personal Information is stored, and storage in computer files that can be accessed only by authorised individuals using login names and secret passwords. Parishes, schools, healthcare and welfare agencies of the Diocese are required to do the same. The Diocese will store Personal Information for such a period of time as the Diocese deems necessary.

9. Disclosure of Information

The Diocese does not reveal Personal Information to other organisations other than through the Australasian Catholic Directory which contains:

- contact details of clergy;

- the name of those lay and ordained persons appointed or elected to Diocesan committees and boards; and
- the name and contact details of people in positions of responsibility within Diocesan groups, parishes and associations.

Information contained in the Australasian Catholic Directory is updated annually, with details of clergy and laity no longer holding a position on a Diocesan committee/board or within a Parish removed.

Disclosure of the Personal Information of clergy and associated persons referred to in this policy will only be made, with their consent, to other individuals, agencies or companies outside of the Diocese, unless the Diocese is required to disclose that information by law. In some limited circumstances and providing confidentiality agreements are in place, contractors to the Diocese may have access to Personal Information.

Public Prayers. Information included in public prayers is personal and consideration for the rights of the individual involved must be respected. As far as reasonably practicable the consent of the person to be prayed for will be sought before making it public. If the Diocese is unable to obtain the individual's consent, it will only make the prayer request public if it is able to do so in a manner that protects the identity of the person. A common means of protecting the identity of the person is to only use the first name of the person for whom the prayer is to be offered.

10. Accessing Stored Information

An individual may request access to their Personal Information that is held by the Diocese. Individuals are entitled to this access, except in specific circumstances that are provided for in the Act. To access Personal Information, an individual must make a written request to the Diocesan Privacy Officer at business@lismore.catholic.org.au

11. Accuracy of Information

The Diocese will take reasonable steps to update or correct, as soon as possible, any information in its possession that has previously be submitted that is inaccurate, incomplete, out-of-date, irrelevant or misleading.

12. Consequences of Not Providing Consent

Subject to certain exceptions, the Diocese cannot collect an individual's Personal or Sensitive Information without their consent. If that consent is withheld, the Diocese may be limited in its ability to:

- attend to the individual's healthcare or welfare needs;
- attend to the individual's child's educational needs;
- attend to pastoral care or other ministry needs that the individual may have;
- offer the individual employment; and
- deal with any inquiries, difficulties or concerns that the individual may have.

13. Notifiable Data Breaches

13.1. Examples of Notifiable Data Breaches

Notifiable Data Breaches *may* include:

- Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information;
- Unauthorised access to personal information by an employee;
- Inadvertent disclosure of personal information due to 'human error', for example when an email is sent to the wrong person; and

- Disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

13.2. Notification of Eligible Data Breaches

The Act contains a Notifiable Data Breach (**NDB**) Scheme that requires the Diocese to notify affected individuals and the Australian Information Commissioner (**OAIC**) about Eligible Data Breaches. If it is not clear that a suspected data breach meets these criteria, the Diocese is required to conduct an assessment to determine whether the suspected data breach is an Eligible Data Breach.

13.3. Initial Process for Suspected Data Breaches

If a suspected Eligible Data Breach is identified by a Worker, or the Diocese is otherwise alerted the following steps should be followed:

Step 1 What should the Worker do?

a. Immediately notify the Privacy Officer of the suspected data breach (see **section 14**).
b. Record and advise the Privacy Officer of the time and date of the suspected breach, the nature of Personal Information involved, the cause and extent of the suspected breach, and the context of the Personal information that forms the basis for the suspected breach.

Step 2 What should the Privacy Officer do?

a. Determine whether a data breach has or may have occurred (see **section 13.5**).
b. Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (**Response Team**) or if not serious the Privacy Officer may decide to deal with the breach.
c. If the breach is serious it must immediately be escalated to the Response Team.

Step 3 Alert the Response Team

a. Privacy Officer convenes Response Team

13.4. Notifiable Data Breach (NDB) Response Team

The Response Team consists of the following personnel:

a. Diocesan Business Manager
b. Privacy Officer
c. HR/WHS Manager
d. Safeguarding Manager
e. ICT Manager

13.5. Assessing Data Breaches

The Privacy Officer is required to consider the following when deciding whether to escalate the matter to the Response Team:

a. Are multiple individuals affected by the breach or suspected breach?
b. Is there a real risk of serious harm to the affected individual(s)?
c. Does the breach or suspected breach indicate a systemic problem in Diocesan processes or procedures?
d. Could there be media or stakeholder attention as a result of the breach or suspected breach?

If yes to any of the above questions, the matter should be escalated to the Response Team.

13.6. Role of Team Response

Step 1 Contain the breach and conduct a preliminary assessment

a. Convene a meeting of the Response Team;
b. Immediately contain breach e.g. :
   - ICT to implement response plan, if relevant;
   - building security to be alerted, if relevant;
   - provide ongoing updates on key developments to the Diocesan Business Manager.
c. Preserve evidence that may be required to ascertain the cause of the breach or assist the Diocese to take corrective action;
d. Develop a communications or media strategy.

Step 2 Evaluate any risks associated with the breach

a. Conduct initial investigation and collect information about the breach including:
   - the date, time, duration, and location of the breach;
   - the type of Personal Information involved in the breach;
   - how the breach was discovered and by whom;
   - the cause and extent of the breach;
   - a list of the affected individuals, or possible affected individuals;
   - the risk of serious harm to the affected individuals; and
   - the risk of harm to others.
b. Determine the context of the collection of the Personal Information;
c. Establish the cause and extent of the breach;
d. Assess priorities and risks based on available information;
e. Maintain appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.

Step 3 Notification

a. Determine who needs to be made aware of the breach (internally and externally);
b. Determine whether to notify impacted individuals – if there is a real risk of serious harm to the affected individuals they should be notified. If there is a high level of risk to the individual because of the breach, then they should be notified immediately.
c. If there is a notifiable data breach, notify OAIC using the Notifiable Data Breach Form at https://www.oaic.gov.au/NDBform.
d. Consider whether others should be notified, including police or other agencies or organisations impacted by the breach (e.g. Australian Taxation Office if there is a breach relating to Tax File Numbers), or where the Diocese is contractually required to do so or has another obligation to notify specific parties.

Step 4 Prevent future breaches

a. Investigate and ascertain the cause of the breach;
b. Report to the Diocesan Business Manager on findings, outcomes and recommendations to prevent a recurrence of the breach including without limitation, revising policies and procedure, providing training to Workers and consider an audit to ensure recommendations are implemented.

13.7. Relevant Timeframes

Upon receipt of written notification of a suspected data breach, the Privacy Officer (together with the Response Team if applicable), must complete enquiries and respond to the notification within 30 calendar days.

14. Concerns about Handling of Personal Information

If an individual has any queries about this policy or wishes to express a concern about the manner in which the Diocese has handled their Personal Information, including where an individual suspects that there has been a data breach, they should contact the Privacy Officer at:

Email: business@lismore.catholic.org.au
Tel: 02 6621 9444
Post:
Privacy Officer
Catholic Diocese of Lismore
PO Box 1
LISMORE NSW 2480

Provided the Diocese has all the necessary information required to adequately investigate a concern, the Diocese will endeavour to respond to the individual who has lodged the concern within 30 calendar days. Should further information be required in order to investigate and respond to a concern, the Diocese may require that information to be provided before it can progress the concern.

15. Office of the Australian Privacy Information Commissioner (OAIC)

Individuals may raise their concerns directly with the Office of the Australian Information Commissioner (**OAIC**) using the following contact details:

Postal Address: GPO Box 5218, SYDNEY NSW 2001
Telephone: 1300 363 992
Facsimile: 02 9284 9666
Email: enquiries@oaic.gov.au

BREACHES OF THIS POLICY

Breaching this Policy may result in disciplinary action, which may include the termination of employment or engagement and, notification to external agencies including without limitation professional standards associations, regulatory agencies and police.

REVISION/ MODIFICATION HISTORY

Date	Version	Current Title	Summary of Changes	Approval Date	Commencement Date
1 May 2020	1	Privacy (Internal) Policy	Initial Policy	15 June 2020	1 July 2020

APPROVAL DATE/ REVISION HISTORY

Approved by: Bishop Gregory Homeming
Date: 15 June 2020
To be revised: 1 July 2023