**Catholic Diocese of Auckland Faith Communities (Parishes/Chaplaincies/ Communities)**

**Privacy Policy**

## 1. Introduction

The Catholic Diocese of Auckland ("Diocese") is committed to promoting and protecting the privacy of all individuals associated with its Faith Communities, Staff Members, Parishioners, Community members, Visitors, Donors and Contractors, and any others. This policy seeks compliance with the Privacy Act 2020, which came into force on 1 December 2020, and the Information Privacy Principles. The Privacy Act describes how we may collect, use, store personal information and the requirements around breaches. The Office of the Privacy Commissioner is empowered by the Privacy Act 2020 to administer, monitor and enforce compliance. Among the many functions of the Privacy Commissioner's Office is that of investigating any alleged breaches and non-compliance of the Privacy Act.

This policy is particularly pertinent to the maintenance and protection of sacramental registers, archives, fundraising or financial giving and parish rolls as these contain sensitive personal information of parishioners and community members.

The Parish Priest or Community Leader is the first point of contact regarding requests for personal information at parish/community level.

The Diocese has a Privacy Officer who understands the Privacy Act and the collection and storage requirements of personal information and can be referred to by parishes. NZCBC also has a National Privacy Officer, who provides advice to the Diocesan Privacy Officer and liaises with the Privacy Commissioner if there are any breaches and/or investigations.

## 2. Purpose

To provide guidance on the following aspects of managing personal information:

- how we collect and store personal information
- what personal information we collect
- how we use and disclose personal information about individuals
- how individuals may access personal information relating to them that is held by the Faith Community
- how personal information is disposed
- how to address complaints of beaches of privacy

- how we respond to the requirements of the Privacy Commissioner and the Privacy Act 2020.

It is important that staff and volunteers understand the Diocese's information management, privacy and confidentiality guidelines.

## 3. Scope

This Policy covers Parishes/Chaplaincies/Communities and their respective Staff Members and Volunteers contracted to perform activities for the Parish, Chaplaincy, Community and those who hold positions on committees and councils that comprise the administrative and pastoral structure of the Parish/Chaplaincy/Community.

## 4. Policy Statement

The Privacy Act 2020 is primarily concerned with the protection of personal information and good information handling practices.

Faith Communities are responsible for ensuring these guidelines and practices are followed through their processes and/or procedures. The following guidelines apply these privacy principles:

### A. Guidelines for collecting, using, accessing, correcting and storing personal information

(The number in brackets [ ] after each guideline refers to the relevant information privacy principle.)

- When we collect personal information about an individual, we make known the purpose of collecting it, who will have access to it, and whether it is compulsory or optional information. We advise that individuals have the right to request access to, and correction of, their personal information.
- We only collect personal information:
    - for purposes connected with the function of the entity, and only when it is necessary to have this information [1]
    - directly from the person concerned, or, if a minor, their parent or guardian, unless it is publicly available from elsewhere, or the person's interests are not prejudiced when we collect the information from elsewhere [2]
    - in a transparent and respectful manner. [1,3,4]
- We have reasonable safeguards in place to protect personal information from loss, unauthorised access, use, or disclosure. These safeguards include the use of individual logins for computers, and lockable filing cabinets. We may require volunteers and third-party contractors to sign confidentiality agreements. [5]
- If an individual wants access to information we hold about them, we provide it. Individuals may request correction of this information or, when not corrected, that a record of the request is attached to the information. [6,7]

- We take reasonable steps to make sure personal information is correct, up to date, relevant and not misleading. [8]
- We only keep information for as long as it is needed, and for the purposes for which it was obtained. [9]
- Information is only used for the purposes for which it was obtained except in certain circumstances (for example, for statistical purposes where the person's identity is not disclosed). [10]
- We safeguard people's information and we do not release that information to third parties unless we are allowed, or required, to release information by law. This covers disclosure to persons other than those able to legitimately access material about others (such as a guardian of a minor).
- As a general rule, information about any person is not given to a third party without the person's knowledge, unless:
    - the information is already publicly available
    - it is being passed on in connection with a purpose for which it was obtained
    - the right to privacy is over-ridden by other legislation
    - it is necessary for the protection of individual or public health and safety. [11]

## B. Guidelines for Legal Holds: preserving records during litigation or investigations

When litigation, an audit, or investigation occurs or is reasonably anticipated, a written notice (referred to as a "Litigation Hold Notice" or "Legal Hold") will be issued to appropriate staff. All records, whether official records, information copies, working documents, or transitory records, potentially relevant to the matter must be retained until the Litigation Hold is terminated. The effect of this notice is to freeze or suspend the destruction or alteration of records, electronically stored information, and other materials identified in the notice.

The Motu Proprio by Pope Francis, *Vos Estis Lux Mundi*, Article 2, §2 also provides for data protection in relation to complaints of sexual abuse matters.

Records relevant to the matter may not be destroyed - even if the retention period in relevant Records Disposal Schedules have expired or expires during the Litigation Hold - until the action is resolved and a notice terminating the Hold has been issued. There are serious legal consequences for individuals that destroy or alter records under a Litigation Hold or know of a pending issue and do not halt destruction.

## C. Guidelines for privacy breaches

Privacy breaches are the loss of personal information to a third party that has no right to that information. If a privacy breach in identified, the first step is to report to your Parish

Priest/manager/faith community leader and they should then report it to the Diocesan Privacy Officer.

The Privacy Officer will work through four steps:

- Contain the breach and make a first assessment
- Evaluate the breach
- Notify affected people if necessary
- Prevent the breach from happening again

If a privacy breach has caused (or is likely to cause) serious harm, the Diocesan Privacy Officer will inform the National Privacy Officer, who will need to notify the Office of the Privacy Commissioner and affected individuals as soon as possible. Under the Privacy Act 2020, it is an offence to fail to inform the Privacy Commissioner when there has been a notifiable privacy breach.

The threshold for a notifiable breach is 'serious harm'. This can be assessed by considering, for example, the sensitivity of the information lost, actions taken to reduce the risk of harm, the nature of the harm that could arise, and any other relevant matters.

## D. Guidelines for compliance notices

Under the Privacy Act 2020, the Privacy Commissioner will be able to direct agencies to provide individuals access to their personal information. The National Privacy Officer is responsible for liaising with the Privacy Commissioner and any relevant entity should a compliance notice be received.

## E. Guidelines for websites

The websites of Faith Communities must be compliant with the Privacy Act 2020. The following guideline is provided as a template to inform website visitors about their privacy rights:

> If you access our website, we may collect additional personal information about you in the form of your IP address and domain name.
>
> Our website uses cookies. The main purpose of cookies is to identify users and to prepare customised web pages for them. Cookies do not identify you personally, but they may link back to a database record about you. We use cookies to monitor usage of our website and to create a personal record of when you visit our website and what pages you view so that we may serve you more effectively.
>
> Our website may contain links to other websites or usage of third-party websites. We are not responsible for the privacy practices of linked websites and linked websites are not subject to our privacy policies and procedures. We are not responsible for risks and liabilities when engaging in any third-party websites like

Facebook, Twitter or Google. Please refer to the Terms of Use on individual websites for further details.

We reserve the right to amend this privacy policy from time to time in order to ensure that it complies with current legal requirements, or in order to implement any changes to our functions and activities.

---

**Policy Approval**

This policy was recommended to Diocesan Faith Communities by the Diocese.

It was adopted by St Luke's Parish Flat Bush on 1 May 2021. Next review due 1 May 2022.