

CATHOLIC ARCHDIOCESE OF WELLINGTON

PRIVACY

A Guide to Privacy for Parishes





Contents

Introduction	01
Applicable Canons for Privacy	02
Civil Law	05
Privacy Act 2020	05
13 Information Privacy Principles	05
Parish Responsibilities	10
General	10
Parish Privacy Officer	11
Privacy Training	11
Privacy Policy	11
Collecting personal information	12
Privacy Disclaimer	12
Privacy Statement	12
Privacy and event management	13
Disclosure of personal information	13
Request to access personal information	13
Sacramental information	13
Privacy breaches and incidents	14
Social Media	16

INTRODUCTION

The Privacy Act, which came into effect on 1 December 2020, has a range of implications for the Catholic Church of Aotearoa, New Zealand. These implications affect how the Church continues to collect and use personal information, and the rights our Catholic community members have to the protection of their own personal information.

The Privacy Act 2020 requires every New Zealand organisation, and organisations who operate in New Zealand, to be compliant with New Zealand privacy law. The Act governs the collection, use, storage, access and disposal of personal information held by an organisation. The Act recognises the shift from a predominantly paper-based world to a digitised one, where sensitive information can be accessed and made public through the internet and social media in an instant, requiring the law to catch up with technological advancements.

We are a Catholic organisation and our moral responsibilities and duties go much deeper than any civil law responsibility. As Catholics, we believe that we are all made in the image of God and therefore every human being deserves to be treated with respect and dignity.

*“So in everything, **do to others what you would have them do to you**, for this sums up the Law and the Prophets.”*

Matthew 7:12

Indeed the right to privacy is protected not only in civil law but also in the Code of Canon Law. This guide is meant to assist those working in parishes who handle personal information. The guide is a basic introduction and there may still be aspects that have not been covered in this guide. If there are any questions, please feel free to contact the Privacy Officer at the Archdiocese of Wellington for assistance.

Review: Version 1.0

[October 2024]

CANONS

APPLICABLE CANONS

FOR PRIVACY

The Code of Canon Law 1983 is the law that governs the universal Catholic Church and every member of the Christian faithful. The right to privacy and protection of reputation is articulated in canon 220, while canon 221 provides an avenue of recourse for those who need to vindicate those rights.

Canon 220

No one is permitted to harm illegitimately the good reputation which a person possesses nor to injure the right of any person to protect his or her own privacy.

Canon 221.

§1. The Christian faithful can legitimately vindicate and defend the rights which they possess in the Church in the competent ecclesiastical forum according to the norm of law.

§2. If they are summoned to a trial by a competent authority, the Christian faithful also have the right to be judged according to the prescripts of the law applied with equity.

The revised "Book VI: Penal Sanctions in the Church," outlines how penal sanctions are applied, including application to those who injure the good name of a member of the Christian faithful.

Canon 1390.

§ 1. A person who falsely denounces a confessor of the offence mentioned in can. 1385 to an ecclesiastical Superior incurs a *latae sententiae* interdict and, if a cleric, he incurs also a suspension.

§ 2. A person who calumniously denounces some other offence to an ecclesiastical Superior, **or otherwise unlawfully injures the good name of another**, is to be punished according to the provision of can. 1336 §§ 2-4, to which moreover a censure may be added.

Canon (noun).

**AN ECCLESIASTICAL RULE
OR LAW ENACTED BY A
COUNCIL OR OTHER
COMPETENT AUTHORITY.**

Image Source: Christchurch Diocesan Archives



CIVIL LAW

THE PRIVACY ACT 2020

Personal Information

(noun).

**PERSONAL INFORMATION IS
ANY PIECE OF INFORMATION
THAT RELATES TO A LIVING,
IDENTIFIABLE PERSON.**

Canon law protects an individual member of the Christian faithful's right to privacy. Civil law in New Zealand protects the personal information of individuals who choose to share their information with the Church. It is important to remember that all organizations, that collect or use personal information in New Zealand, are required to be compliant with the Privacy Act 2020.

The Privacy Act 2020 outlines 13 Information Privacy Principles to guide organisations in the collection, holding, use and disclosure of personal information.

These principles are

1. PURPOSE

Organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose. This principle is based on the concept of data minimization. If you do not need it, do not collect it.

2. SOURCE

Personal information should be collected directly from the person it is about. The best source of information about a person is usually the person themselves. There are certain situations when organisations can collect from others — with their consent; where information is publicly available or where direct collection is not practicable.

3. COLLECTION

Organisations should be open about what happens to the personal information once it has been collected. This principle is based on helping a person understand the reason you are collecting their information — why it is being collected, who will see it and what will happen if it is not provided.

4. MANNER

Personal information must be collected in a way that is lawful and seen as fair and reasonable in the circumstances. What is fair depends on the circumstances, like the individual's age and capacity and the sensitivity of the information. Circumstances, such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected should also be taken into account. You need to take particular care when collecting information from children and young people.

5. SECURITY

Organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information.

6. ACCESS

People have a right to access their own information, and generally an organization must provide access to that information when requested by an individual. People can only ask for information about themselves. The Privacy Act does not allow you to request information about another person, unless you are acting on that person's behalf and have written authorisation. In some situations, an organisation may have good reason to refuse a request for access to personal information. For example, the information may involve an unwarranted breach of someone else's privacy, or releasing it may pose a serious threat to someone's safety.

7. CORRECTIONS

An individual has a right to ask an organisation to correct information about them if they think it is wrong. If an organisation does not agree that the information needs correcting, an individual can ask that an organisation attach a statement of correction to its records, and the organisation should take reasonable steps to do so.

8. ACCURACY

Personal information should be checked for accuracy before it is used or disclosed, ensuring it is up to date, complete, relevant and not misleading.

9. RETENTION

Organisations should not keep personal information for longer than it is required for the purpose it may lawfully be used. Organisations that have a *Records Retention and Disposal Schedule* in place should adhere to the provisions laid out in the schedule.

10. USE

Organisations can generally only use personal information for the purpose it was collected. Sometimes other uses are allowed, such as use that is directly related to the original purpose, or if the person in question gives their permission or consent for their information to be used in a different way.

11. DISCLOSURE

An organisation may generally only disclose personal information for the purpose for which it was originally collected or obtained. Sometimes other disclosure is allowed, if directly related purpose, or if the person in question gives their consent for the disclosure.

For instance, an organisation may disclose personal information when:

- disclosure is one of the purposes for which the organisation got the information
- the person concerned authorises the disclosure
- the information is to be used in a way that does not identify the person concerned
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to uphold or enforce the law.

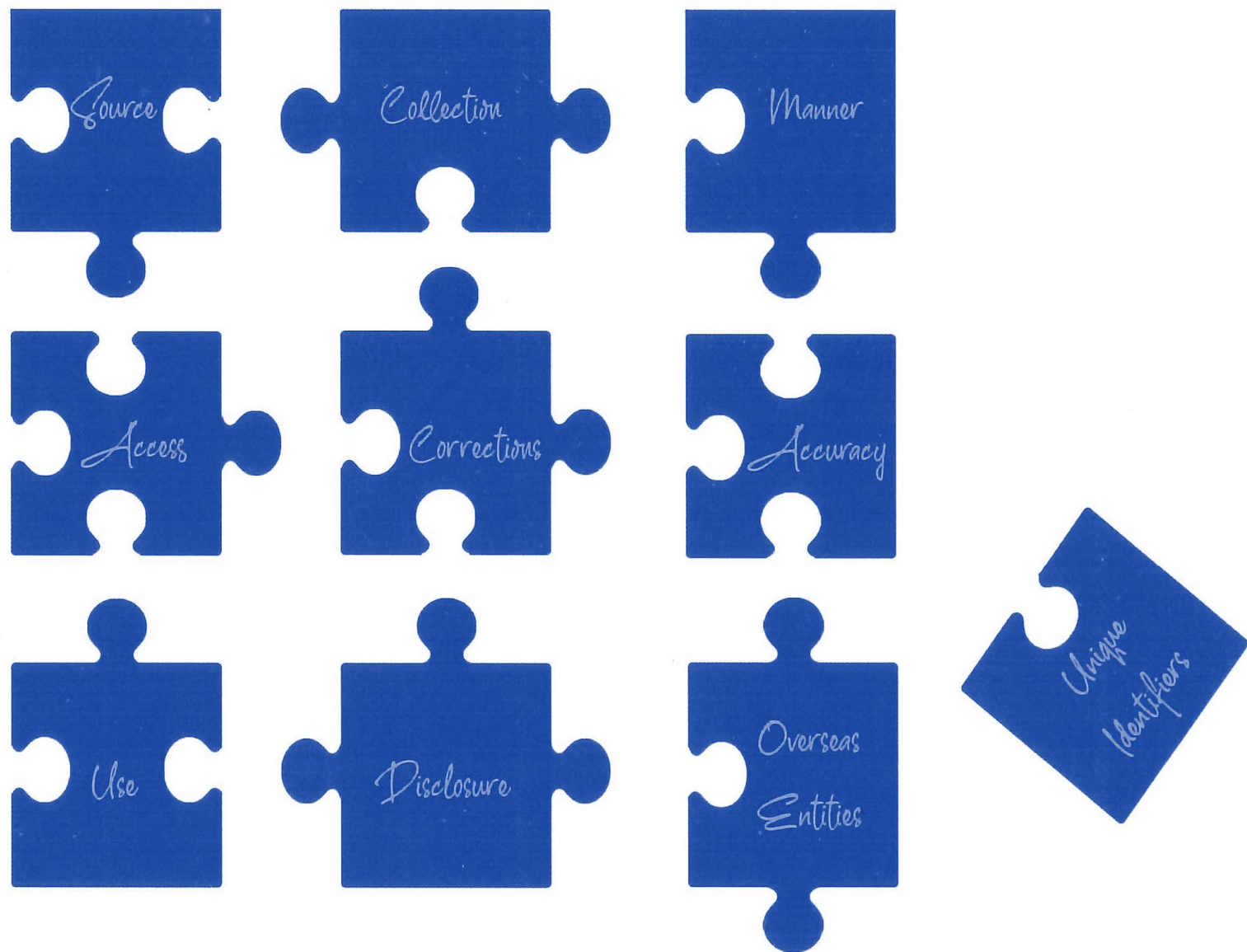
12. OVERSEAS ENTITIES

Personal information should only be sent overseas from New Zealand if the overseas entity does business in New Zealand and is subject to the Privacy Act 2020, or has comparable privacy protection.

13. UNIQUE IDENTIFIERS

Unique identifiers should only be used to identify people's personal information when it is clearly allowed.





THE 13 INFORMATION PRIVACY PRINCIPLES AS OUTLINED IN THE PRIVACY ACT 2020 (PART 3, S22) FURTHER INFORMATION AT [HTTPS://WWW.PRIVACY.ORG.NZ/PRIVACY-ACT-2020/PRIVACY-PRINCIPLES/](https://www.privacy.org.nz/privacy-act-2020/privacy-principles/)



PARISH RESPONSIBILITIES

GENERAL

The protection of the right to privacy is important to the life of the Church, and parishes should work to educate our faith communities in the use, and misuse, of personal information, which should be reflected in all parish policies, procedures, and communications.

Through good governance and accountability for all of Christ's faithful, and parishes should proactively protect each individual, which ensures the protection of the entire flock entrusted to our priests .

The New Zealand Catholic Bishops Conference (NZCBC) has appointed a National Privacy Officer. In addition to overseeing privacy in the work of NZCBC, they support and mentor the Diocesan Privacy Officers in each of our 6 dioceses and some NZCBC entities. The Diocesan Privacy Officers in turn support parishes who, as best practice, will also have someone responsible for privacy in their parish. If you have any concerns about privacy you are welcome to contact the appointed Archdiocesan Privacy Officer,

**“WE SHOULD
PROACTIVELY ENGAGE
TOGETHER, FOR WE DO
NOT WALK ALONE BUT IN
COMMUNIO AS ONE
CHURCH. “**

*E. Ong, New Zealand Privacy Law in Relation to Canon Law,
The Canonist Vol 11 No 2 246 - 274.*

PARISH PRIVACY OFFICER

The Privacy Act requires organisations to have at least one person who fulfils the role of privacy officer in each organisational entity. Each parish is considered an organisational entity; a juridic person under Canon Law. Each parish should assign this responsibility and liaise with the Diocesan Privacy Officer for advice and guidance as needed.

The parish privacy officer should be a responsible and practical person, familiar with the principles in the Privacy Act, who will work to make sure the parish complies with the Act in all activities. The officer's role will include:

- raising awareness about privacy among parish staff, volunteers, and others involved in ministry
- ensuring policy and procedures are set out and enforced
- being contacted about and responding to privacy breaches

PRIVACY TRAINING

Free privacy Training should be available as part of a professional development programmes for Parish staff, with responsibility for privacy. Additionally the Archdiocesan Privacy Officer can run specific training for a parish office on request.

Online training is available on the Office of the Privacy Commissioner's e-learning website. <https://elearning.privacy.org.nz/>

There are also numerous blog posts and podcasts from the Office of the Privacy Commissioner around the key changes to Privacy legislation. <https://www.privacy.org.nz/privacy-act-2020/resources/>

PRIVACY POLICY

Each Parish should have a Privacy Policy. A privacy policy document should provide guidance on the following aspects of managing personal information:

- how the parish collects and stores personal information
- what personal information a parish will typically collect
- how a parish will use and disclose personal information about individuals
- how individuals may access personal information relating to them that is held by **the parish**
- how personal information is disposed
- how to address complaints of breaches of privacy
- how the parish responds to the requirements of the Privacy Commissioner and the Privacy Act 2020

A policy template is available from the Archdiocesan Privacy Officer and can be used to provide high level guidance on how personal information should be collected, used, disclosed and retained. All administration staff and volunteers who receive or have access to personal information should be aware of the Privacy Policy requirements.

It is important that all parish staff, paid or unpaid, understand all parish information management, privacy and confidentiality guidelines.

**THE PRIVACY ACT DOES
NOT APPLY TO PERSONAL
INFORMATION COLLECTED
FROM A PUBLICLY
AVAILABLE SOURCE**

COLLECTING PERSONAL INFORMATION

Administrative procedures around the collection, handling and use of personal information should be captured in procedure documents to ensure consistency across all parish staff.

PRIVACY DISCLAIMER

Any time personal information is collected a privacy disclaimer, indicating purpose of collection, use, access and retention, should be included when collecting. This includes Parish Enrolment forms, Parish Census Forms or Enrolment for Sacramental Programmes.

Here is an example of a privacy disclaimer:

By completing this form, I consent to my information being stored and used for the pastoral, financial, administrative and fundraising purposes of the [insert name of parish] and the Catholic Archdiocese of Wellington. I understand that my data will be held securely and that I have a right to access my information. I understand that when this information is no longer required for this purpose, my data will be disposed of according to the Parish and Diocesan Record Retention and Disposal procedure.

PRIVACY STATEMENT

If someone wants more specific information about the collection and use of the personal information the parish should have a privacy statement ready. This statement should explain the purpose for collecting the personal information, how it will be used, to whom it will be disclosed, the storage of the information and a person's right to access or amend it.



PRIVACY AND EVENT MANAGEMENT

If you are holding a parish event it is important to consider any privacy implications associated with the registration and documentation of the event. Registration forms should be accompanied by a disclaimer clearly explaining the purpose of collecting the information required, how it will be used and how long it will be retained.

If the parish wishes to record the event (through film or photographs) you must let attendees know. As it is a 'public' event it is not necessary to obtain consent from everyone in attendance. However, it is good privacy practice to give attendees the option to not be photographed or captured on film, or have images published. This can be achieved by placing signs at every entrance or to identify the photographer should anyone wish not photographs to be published.

Here is an example of signage that could be used:

*Please be aware we are taking photographs at this public event which may be used for publication (online and print). If you do not consent to photographs of you being published please identify yourself to the photographer or let one of the parish team know.
Your privacy is important to us, so if you have any concerns please let us know.*

DISCLOSURE OF PERSONAL INFORMATION

In accordance with the Privacy Act, personal information collected by the parish must not be disclosed to third parties, unless a privacy disclaimer at the time of collection has clearly identified with whom personal information may be shared, or unless you have the consent of the individuals concerned.

If you have any concerns about whether personal information can be disclosed please contact the Archdiocesan Privacy Officer for clarification.

REQUEST TO ACCESS PERSONAL INFORMATION

The Privacy Act Information Privacy Principle #6 states that people have a right to ask for access to their own personal information.

People can only ask for information about themselves. The Privacy Act **does not** allow a person to request information about another person, unless their are acting on that person's behalf and have written permission.

It is useful to receive requests for access to personal information in writing, clearly stating what information they are seeking to access.

SACRAMENTAL INFORMATION

Care must be taken to protect the privacy of individual parishioners. While sacramental records contain information about public events, they also contain confidential and personal information. Sacramental details must not be given to a third party without the consent of the subject of the sacrament.

PRIVACY BREACHES AND INCIDENTS

Organizations that deal with the collection, handling, or disclosure of personal information may be at risk of a privacy incident or breach. Whether intentional, or accidental, instances will occur where personal information is at risk of inappropriate access, use or disclosure.

Anytime a risk to personal information is discovered, the incident, should be reported to the Parish Privacy Officer. Then the risk can be mitigated, and the likelihood of a more serious privacy breach occurring is reduced.

The main actions when an incident is discovered is to **Limit** further disclosure, **Report** to parish and diocesan privacy officers, **Assess** the extent of risk, **Prevent** to ensure the risk does not reoccur.

All incidents and breaches should be reported to the Archdiocesan Privacy Officer.

CYBER SECURITY BREACHES AND INCIDENTS

Cyber security incidents such as hacking, malware attacks and security breaches are becoming more common. It is important that all online data is protected and secure.

If the parish is exposed to a cyber security incident it is important to identify and fix the problem and put steps in place to prevent it from happening again. **All cyber security incidents** should be reported to the Archdiocesan Privacy Officer.

Sleep Cycle



Facebook

In

BBC

S O C I A L M E D I A

GENERAL

The Catholic Archdiocese of Wellington recognizes that in today's environment, use of social media and other networking and communication technologies and applications assist in the pastoral and evangelical mission of our church. Parishes are encouraged to use social media and technologies to accomplish their ministry.

The Archdiocese also has an obligation to ensure responsible and safe use of these technologies, reflective of the teaching and mission of the Catholic Church. Online engagement with others should facilitate a growing relationship with Christ.

Procedures around the use of Social Media should be similar to that of a publication when it comes to images or video of parishioners. Consent must be obtained from those photographed or recorded.

When organizing or facilitating programmes or activities where photographs or video footage of children (those under 16 years of age) or vulnerable adults are to be taken, privacy concerns should be considered. This includes gaining the written consent of the parent or caregiver of the child and for a vulnerable adult, the adult can give their consent if they are able to do this, or the consent of their caregiver.

In the use of photographs, particularly of youth, the subjects should not be identified by more than a first name and parishioners and minors should not be tagged in the posts.

Care should be taken when sharing posts from other pages. If the parish chooses to share posts from parishioners' personal accounts, permission to share should be obtained first.



ARCHDIOCESE OF WELLINGTON