

**CATHOLIC
DIOCESE OF HAMILTON**

PRIVACY!

**A GUIDE TO PRIVACY
FOR PARISHES**



CONTENTS:

Contents	1
Introduction	2
Applicable Canons	3
Civil Law & The Privacy Act	5
The 13 Privacy Principles	9
Parish Responsibilities	10
General	10
Privacy Officer	11
Privacy Training	11
Privacy Policy	11
Collecting Personal Information	12
Privacy Disclaimer	13
Privacy Statement	13
Privacy Event Management	13
Disclosure of Personal Information	14
Request to Access Personal Information	14
Sacramental Information	14
Privacy Breaches and Incidents	15
Cyber Security Breaches and Incidents	15
Social Media	16

INTRODUCTION

The Privacy Act 2020 (the 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 right of our Catholic Community members to have their personal information protected.

The Privacy Act 2020 requires every New Zealand agency and entity that operates 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 agency. The Act recognises the shift from a predominantly paper-based world to a digitised one, where sensitive information can be accessed and made public via the internet or social media in an instant - requiring the law to catch up with technological advancements.

We are a Catholic agency, 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 designed to assist those working in parishes who handle personal information. The guide is an introduction only, and some aspects have not been covered. If you have any questions or need assistance, please feel free to contact me, Marian Greene.

Privacy Officer for the Diocese of Hamilton

Applicable Canons

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 that a person possesses nor to injure the right of any person to protect their 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 before an ecclesiastical superior or confessor of the offence mentioned in can.1387 incurs a latae sententiae interdict and, if a cleric, he incurs also a suspension

§ 2 A person who offers an ecclesiastical superior any other calumnious denunciation of a delict or who otherwise injures the good reputation 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



CIVIL LAW & THE PRIVACY ACT 2020

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 organisations that collect or use personal information in New Zealand must comply with The Privacy Act 2020.

This Act outlines 13 Information Privacy Principles to guide organisations in the collection, holding, use, disclosure of and destruction 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 - the information must be necessary for that purpose. This principle is based on the concept of data minimisation. **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 from the person themselves. There are certain situations when organisations can collect this information from others, with the consent of the person to whom it relates, where the information is publicly available, or where direct collection is not practicable.

3. COLLECTION

Organisations should be open about what happens to 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 that is seen to be fair and reasonable in the circumstances. What is fair depends on the circumstances, such as the individual's age and capacity and the sensitivity of the information. Circumstances such as the purpose of the 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 or young people.

5. SECURITY

Organisations must ensure that 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. Generally, an organisation must provide access to the information when requested to do so by the person to whom the information pertains. People can only access information about themselves.

The Privacy Act 2020 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 –

such as (for example) when 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 believe it is incorrect. Suppose an organisation does not agree that the information requires correcting. In that case, 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 to ensure that it is accurate, up-to-date, complete and not misleading.

9. RETENTION

Organisations should not keep personal information for longer than 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 that 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 differently.

11. DISCLOSURE

An organisation may generally only disclose personal information for the purpose for which it was initially obtained or collected. Sometimes another disclosure is allowed, if it is for a 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 received 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

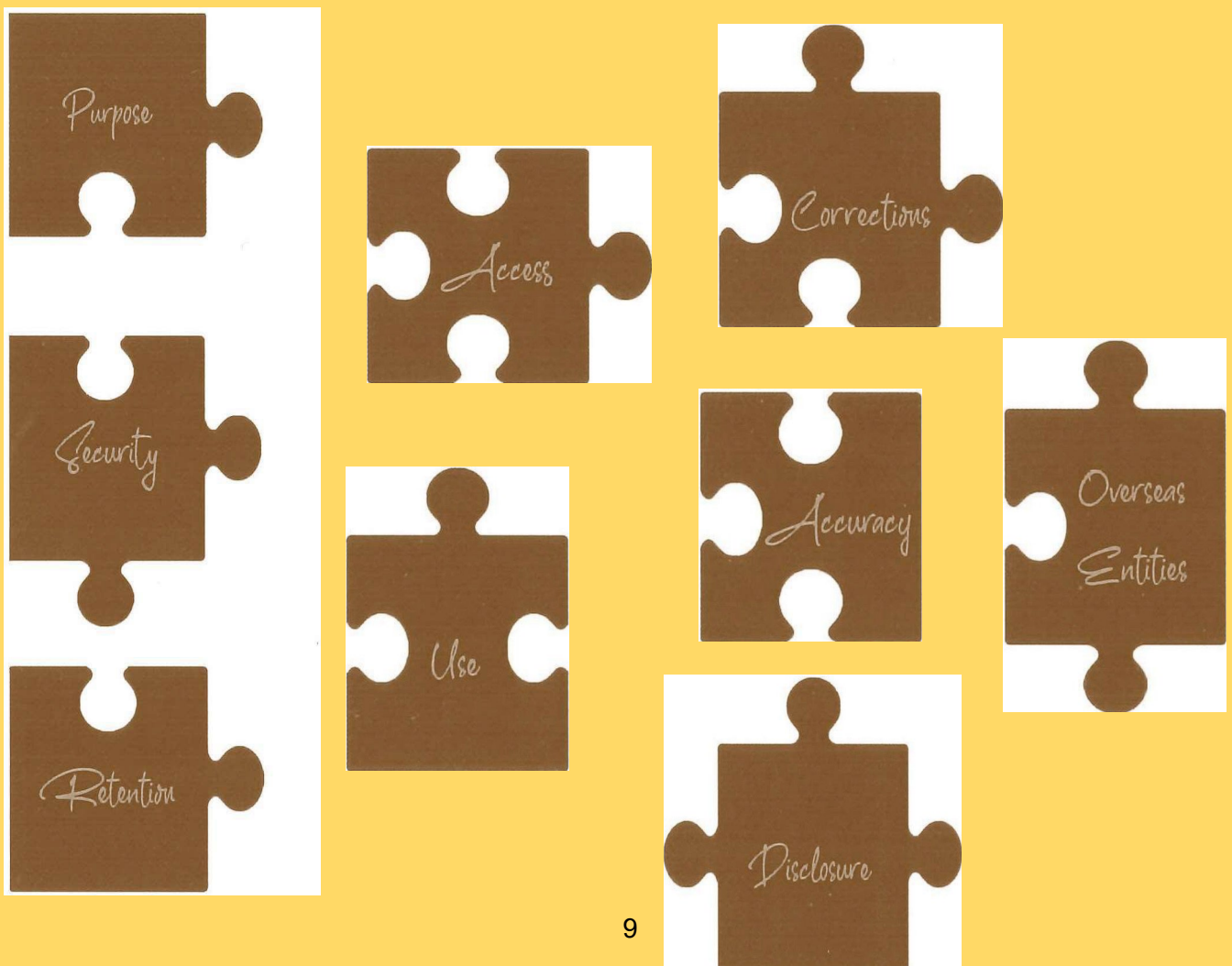
Personal information should only be sent overseas from New Zealand if the overseas agency does business in New Zealand and is subject to the Privacy Act 2020 or has comparable privacy protection.

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)



PARISH RESPONSIBILITIES

GENERAL

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

Through good governance and accountability for all of Christ's faithful, 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 six 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 privacy concerns, you are welcome to contact the appointed Hamilton Diocesan Privacy Officer.

Marian Greene
PH: 07 8566989
E: mariang@cdh.org.nz

"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 their organisational agency. Each parish is considered an organisational agency - a judicial 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 of the Privacy Act, who will ensure 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 programme for parish staff with responsibility for privacy. Additionally, the Diocesan Privacy Officer can run specific training for a parish office on request. Online training is available at the Privacy Commissioner's learning website: <http://www.privacy.org.nz>

There are also numerous blog posts and podcasts around the key changes to the privacy legislation on this site.

PRIVACY POLICY

Each Parish should have a Privacy Policy. A privacy policy document should guide 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 of
- 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 from the Privacy Document Library for parishes 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.

Note: 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

Whenever personal information is collected, a privacy disclaimer, indicating the 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.

An example of a privacy disclaimer can be found in the Privacy Document Library for Parishes.

PRIVACY STATEMENT

To provide more specific information about the collection and use of the personal information on request, 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.

An example of a privacy statement can be found in the Privacy Document Library for Parishes.

PRIVACY AND EVENT MANAGEMENT

If you are holding a parish event, it is essential 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 advise attendees of this. 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 NOT to be photographed or captured on film, or have images published. This can be achieved by placing signs at every entrance, making an announcement at the event, or by identifying the photographer to those present, should anyone wish not to be photographed or not want their photograph published.

An example of appropriate signage can be found in the Privacy Document Library for Parishes.

DISCLOSURE OF PERSONAL INFORMATION

By 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 identified with whom personal information may be shared, or you have the consent of the individual(s) concerned.

If you have any concerns about whether personal information can be disclosed, please get in touch with the Diocesan Privacy Officer for clarification.

REQUEST TO ACCESS PERSONAL INFORMATION

The Privacy Act Information Privacy Principle #6 provides 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 they are acting on that person's behalf and have written permission.

It is essential 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, or their parent in the case of minors.

PRIVACY BREACHES AND INCIDENTS

Organisations 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 that 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 are to limit further disclosure, report to parish and diocesan privacy officers, assess the extent of risk and prevention to ensure the risk does not recur.

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

CYBER SECURITY BREACHES AND INCIDENTS

Cybersecurity incidents such as hacking, malware attacks, and security breaches are becoming more common. All online data must be protected and secure.

If the parish is exposed to a cybersecurity incident, it is essential to identify and fix the problem and implement measures to prevent it from happening again. All cybersecurity incidents should be reported to the Diocesan Privacy Officer.



SOCIAL MEDIA

The Catholic Diocese of Hamilton recognises that in today's environment, the use of social media and other networking and communication technologies and applications assists in the

The pastoral and evangelical mission of our church. Parishes are encouraged to use social media and technologies to accomplish their ministry.

The Diocese also has an obligation to ensure the 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 those of a publication when it comes to images or videos of parishioners. Consent must be obtained from those photographed or recorded.

When organising 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, in the case of a vulnerable adult, the adult themselves (if they are able) or otherwise, 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.



CATHOLIC DIOCESE OF HAMILTON