PRIVACY ACT 2020 SUMMARY

This summary was prepared mid-2022, as a useful reference document for Clubs. Updates may happen from time to time, and the date of update will be included in the title.

All this information can be obtained through the Privacy Commissioner website. **https://www.privacy.org.nz/** As well this site has tools to assist in the generation of a Privacy Statement, and some good resources to reference.

A thorough review of the implications of this act on the way your club operates should be undertaken – how do you collect, distribute, manage, and update members information; who has access to your club records, and are passwords and hardware secure and club specific; how do you deal with complaints or requests about handling of personal information; etc.

INTRODUCTION

A right to privacy can mean a right to be left alone, a right to control who sees information about you, or a right to make decisions about your personal life without government intervention. The value of a right to privacy can also vary depending on circumstances, cultural context, time and personal preference. Although privacy is important, it is not absolute, as in some instances social interests can be more important - such as preventing crime, ensuring safety, and ensuring that courts get information to make their decisions.

On 1 December, the Privacy Act 2020 came force and became New Zealand's main privacy law. It applies to any person, organisation, or business whether it's in the public sector or private sector, that collects and holds personal information about other people, and includes everything from Government Agencies to social clubs. The Act includes 13 principles that guide how personal information can be collected, used, stored, and disclosed. As well, The Office of the Privacy Commissioner (OPC) works to develop and promote a culture in which personal information is protected and respected.

The Privacy Principles

Collecting Personal Information - when, where, and how you can collect it.

Principle 1 - Purpose for collection of personal information
Principle 2 - Source of personal information - collect it from the individual
Principle 3 - Collection of information from subject - what to tell the individual
Principle 4 - Manner of collection

Holding personal Information - People have a right to access and correct their personal information.

Principle 5 - Storage and security of information
Principle 6 - Access to personal information
Principle 7 - Correction of personal information

Using and Sharing Information - Make sure information is accurate, and used appropriately.

Principle 8 - Accuracy of personal information
Principle 9 - Retention of personal information
Principle 10 - Limits on use of personal information
Principle 11 - Disclosure of personal information
Principle 12 - Disclosure outside New Zealand
Principle 13 - Unique identifiers

Having a privacy officer

The Act requires all agencies to have at least one person who's familiar with the agency's privacy obligations and fulfils the role of a privacy officer.

Collecting personal information

1. Only collect information you need

Principle 1 states that 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 about data minimisation. If you're thinking about collecting personal information, the first thing you should consider is why you're collecting it - what are you're trying to achieve by collecting the information. The more unnecessary information you have, the more will be needed to be kept up to date, and the more likely mistakes are to happen.
If the personal information you are asking for isn't necessary to achieve something closely linked to your organisation's activities, you shouldn't collect it.

If your purpose changes or you want to use the personal information you have collected for an unrelated purpose, you are likely to need the agreement of the people you collected it from.

2. **Collect information directly from the person**

Whenever you get personal information deliberately, you are 'collecting' it. Personal information should be collected directly from the person it is about and collecting information from the person concerned means they know what is going on and have some control over their information. They will know what you've got and what you're doing with it

- they're far less likely to be surprised or upset.

Organisations can collect it from other people in certain situations. For instance:

- if the person concerned authorises collection from someone else,
- if the information is collected from a publicly available source
- if collecting information from the person directly is not really practicable or would undermine the purpose of collection.

Sometimes, information can be collected from other sources for law enforcement and court proceedings.

3. **Tell people what you're doing**

Organisations should be open about why they are collecting personal information and what they will do with it. This principle is about helping people understand the reasons you are collecting their information. The best way to do this is with a clear privacy statement. When an organisation collects personal information, it must take reasonable steps to make sure that the person knows:

- that you're collecting their information
- why you're collecting their information
- whether you're collecting their information under a particular law
- who will be able to access the information
- whether they can choose not to give you the information
- what will happen if they don't give you the information
- that they can ask to access and correct their personal information
- how to contact you, or any organisation that is holding their information for you.

Sometimes there may be good reasons for not letting a person know about the collection – for example, if it would undermine the purpose of the collection to protect law enforcement investigations, or it's just not possible to tell the person.

4. Collect information fairly and lawfully

Principle 4 states that personal information must be collected in a way that is lawful, and seen as fair and reasonable in the circumstances.

Circumstances to be considered are the individual concerned (age and capacity), the time and the place it was collected, intrusion on privacy, and the natural sensitivity of the information. Threatening, coercive, or misleading behaviour when collecting information from an individual could well be considered unfair.

Holding personal information

You must keep the personal information you hold safe and secure. You must also give people access to the information you hold about them and take reasonable steps to correct it if it's wrong.

5. **Store personal information securely**

Principle 5 states that organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information. You must make sure that you take reasonable steps to store and use personal information securely. You may need a locked cabinet for physical documents, or password protection for electronic files. Make sure only appropriate people can access the information. Look after information in transit as well, e.g. a secure payments channel for people buying things off your website.

Security includes taking steps to prevent unauthorised or inappropriate access by staff. Have clear policies and guidelines in place that set out acceptable staff behaviour. Depending on the sensitivity of the information, it may be necessary to set up systems that limit or keep track of who accesses it.

If an organisation has a serious privacy breach it must notify the Office of the Privacy Commissioner as soon as possible (within 72 hours).

6. **Give people access to their personal information**

Principle 6 states that people have a right to ask for access to their own personal information. Generally, an organisation must provide access to the personal information it holds about someone if the person in question asks to see it. You should keep personal information in a way that is easily retrievable so you can:

1. confirm that you hold a person's information if they ask
2. give them access to it.

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

If someone asks for access to their personal information, you must respond within 20 working days of receiving the request. Your response should include a decision about whether you will be providing the requested information. It doesn't necessarily have to include the information, but you should provide it as soon as possible afterwards. It's best

provide the information promptly unless there's a reason you can withhold it under the Privacy Act.

In some situations, an organisation may have good reasons 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.

Part 4 of the Privacy Act has a full list of the good reasons for refusing access to personal information, and clarity around how to respond to a request for personal information.

7. Let people correct their personal information

Principle 7 states that a person has a right to ask an organisation or business to correct information about them if they think it is wrong. If you don't think you need to correct the information, you must still record that the person asked you to correct the information, and note exactly what they thought was wrong. Attach that record to the person's file so that everything is together. Knowing what the person thinks will help anyone else who looks at the record to make better decisions.
The rules for how an organisation must respond to a corrections request are set out in Part 4, Subpart 2 of the Privacy Act 2020.

Using and Sharing Information

8. Make sure personal information is accurate

Before you use personal information, check that it's accurate, up-to-date, complete, relevant, and not misleading. Incorrect information isn't any use to you, and it could lead you to make wrong decisions about the person involved.

9. Disposing of personal information

Principle 9 states that an organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used. Your agency can set its own policies. It can be expensive to store and secure large quantities of information. Holding more information means a greater risk of a privacy breach. However, retaining key information can be helpful, for example if a customer returns to your service.
Dispose of personal information securely so that no-one can retrieve it. For example:

- remove names, addresses and birthdates from documents before you dispose of them
- use shredders and secure destruction services

- wipe hard drives from machines – including photocopiers – before you sell or decommission them
- delete back-up files as well as originals.

10. Limits on use of personal information

Organisations can generally only use personal information for the purpose it was collected, and there are limits using personal information for different purposes. Personal information is a useful and valuable commodity. Other people or organisations may want to use personal information you have collected through your organisation, rather than collecting it themselves. However, it is recommend that you only use personal information for the purpose for which you collected it. People get upset if you use their information without their knowledge or permission, and you risk losing their trust.

11. Disclosure of personal information

An organisation may generally only disclose personal information for the purpose for which it was originally collected or obtained. Sometimes other reasons for disclosure are allowed, such as disclosure for a directly related purpose, or if the person in question gives their permission for the disclosure. There are circumstances under which you may be able to use personal information for a new purpose, for example:

- 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. Disclosure outside New Zealand

A business or organisation may only disclose personal information to another organisation outside New Zealand if the receiving organisation:

- is subject to the Privacy Act because they do business in New Zealand
- is subject to privacy laws that provide comparable safeguards to the Privacy Act
- agrees to adequately protect the information, e.g. by using model contract clauses.
- Is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act. The goal is to make sure that the privacy protections that

individuals can reasonably expect under New Zealand's Privacy Act continue to apply when their information is disclosed and used in a different country.

Principle 13 - Unique identifiers

Principle 13 sets restrictions on assigning identifying numbers and other unique identifiers to individuals. The principle states that an organisation can only assign unique identifiers to people when it is necessary for its functions. Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations as a way to uniquely identify the person to the organisation assigning the identifier. Examples include driver's licence numbers, passport numbers, IRD numbers, or National Health Index (NHI) numbers.

An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation. For example, this prevents the Government from giving you one personal number to use in all your dealings with government agencies. However, an organisation can record (and use) a person's unique identifier so that they can communicate with another organisation about the individual.

Organisations must also take reasonable steps to protect unique identifiers from misuse and make sure they verify someone's identity before assigning a unique identifier.

Privacy officers

The Privacy Act requires organisations to have at least one person who fulfils the role of privacy officer.

Who should be a privacy officer?

The person responsible for privacy matters depends on the size of your organisation, the work it does, and what personal information it handles. In smaller organisations, the manager is normally responsible for all legal compliance, including privacy. Whoever takes on the duties of a privacy officer, it's important for managers in the organisation to take their advice seriously.

Why you need a privacy officer

As well as being required by law, having a privacy officer is useful for your organisation. Good privacy builds trust with clients and employees and enhances a business' reputation. An internal privacy adviser who is familiar with the business and privacy law adds value to

your organisation. Privacy officers can prevent or fix privacy issues before they become serious problems. This can save you money, or lost business.
If someone complains that your organisation has breached their privacy, your privacy officer can help resolve things quickly and effectively.

The duties of a privacy officer

A privacy officer will:

- be familiar with the privacy principles in the Privacy Act
- work to make sure the organisation complies with the Privacy Act
- deal with any complaints from the organisation's clients about possible privacy breaches
- deal with requests for access to personal information, or correction of personal information
- act as the organisation's liaison with the Office of the Privacy Commissioner.

They may also:

- train other staff at the organisation to deal with privacy matters
- advise their organisation on compliance with privacy requirements
- advise their organisation on the potential privacy impacts of changes to the organisation's business practices
- advise their organisation if improving privacy practices might improve the business
- be familiar with any other legislation governing what the organisation can and cannot do with personal information.

Resources for complying with the Privacy Act

Best place to go is the Privacy Commissioners website.

Privacy resources for agencies https://www.privacy.org.nz/about-us/introduction/

Development of Privacy Statement https://www.privacy.org.nz/tools/privacy-statement-generator/

From a practical perspective when developing a privacy statement think about all the places names and addresses are used:

Emails
Accounting packages
Programme booklets

Think about usernames and password management

Think about collection of data and its upkeep, where it is stored, who has access to it.

Think about notification of where data will be used and seen – how to manage mail outs, and databases.