PRIVACY OFFICER JOB GUIDELINE AND RESPONSIBILITIES:

Job Title	Privacy Officer
Responsible To	Club President

The Privacy Act 2020 requires organisations to have at least one person who fulfils the role of Privacy Officer. The Privacy Officer is responsible for all legal compliance, including privacy in regards to all club business and membership personal information.

As well as being required by law, a privacy officer is useful for your club to build trust with members, enhance club reputation and add value to your organisation. Privacy officers can prevent or fix privacy issues before they become serious problems saving money, and lost business.

If someone complains that your organisation has breached their privacy, your privacy officer can help resolve things quickly and effectively.

Privacy Officer Duties

A privacy officer will:

- be familiar with the privacy principles in the Privacy Act 2020
- work to make sure the organisation complies with the Privacy Act 2020
- deal with any complaints from within the organisation 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.
- 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 practices
- advise their organisation if improving privacy practices might improve the organisation
- be familiar with any other legislation governing what the organisation can and cannot do with personal information.

1. Collecting Personal Information

Whenever you get personal information deliberately, you are 'collecting' it. The Privacy Act 2020 sets out what personal information you can collect, where you may collect it from and how you may collect

it.

Only collect information you need:

If you're thinking about collecting personal information, the first thing you should consider is why you're collecting it. The Privacy Act 2020 requires that you only collect personal information that's necessary for a lawful purpose.

Your purpose is what you're trying to achieve by collecting the information eg: personal information regarding membership to a club.

Before you collect personal information, think about what information you need to achieve your purpose. You may find you don't need to collect as much as you originally thought, or you may not need to collect any at all. The more unnecessary information you have, the more you have to keep up to date.

If your lawful 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.

Collect information directly from the person:

Generally, you should collect information directly from the person it's about. Then the person will know what information you've got and what you're doing with it.

Sometimes you do need to get information from other sources, to do this you must have the consent of the person the information is about.

Tell people what you're doing:

If you're collecting personal information from someone, you need to let them know what you're doing. The best way to do this is usually with a clear privacy statement.

You need to take reasonable steps to tell people:

- 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 it's obvious to people that you're collecting their information. Other times, it may not be as obvious but whatever the case, being open with people about what you're doing with their information means you won't take them by surprise, and they're less likely to object.

You may not need to tell the person if it would undermine the purpose of the collection, or it's just not possible to tell them.

Collect information fairly and lawfully

Make sure you collect personal information in a way that is lawful, fair and not unreasonably intrusive. For instance, covert surveillance is usually not allowed.

2. Your Responsibilities:

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.

Store personal information securely

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.

Give people access to their personal information

People have a right to access the personal information you hold about them. You should keep personal information in a way that is easily retrievable so you can:

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

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 to provide the information promptly unless there's a reason you can withhold it under the Privacy Act 2020.

You may be able to withhold information if:

- it isn't readily retrievable
- releasing it could negatively affect the requestor's mental health
- releasing it could put somebody else in danger
- releasing it would breach somebody else's privacy
- it was provided in confidence
- you don't have it
- the request is trivial
- the request is vexatious

3. Let people correct their personal information

People can ask you to correct their personal information if they think it's 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.

4. Using and disclosing personal information

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.

5. 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.

6. Don't keep personal information for longer than you need

The Privacy Act 2020 doesn't specify how long you can keep personal information – only that agencies shouldn't keep information for longer than they need it.

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.

7. Disposing of personal information

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.

8. Use information for the purpose you got it

Generally, 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.

There are circumstances under which you may be able to use personal information for a new purpose, for example:

- when you have the permission of the person the information is about
- if it's directly related to the purpose for which you gathered the information
- if it's necessary to uphold or enforce the law.

9. Only disclose personal information if you have a good reason

Be careful about disclosing personal information to people, both inside and outside your organisation. You can only do this in some situations, such as when:

- you have the permission of the person the information is about
- another law requires you to disclose it
- it's one of the purposes for which you got the information
- it's necessary to uphold or enforce the law
- it's necessary for court proceedings
- you disclose it in a form that doesn't identify the person it's about.

10. Sending personal information overseas

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 2020 because they do business in New Zealand
- is subject to privacy laws that provide comparable safeguards to the Privacy Act 2020
- 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.

11. Unique identifiers

A business or organisation may only use a unique identifier (such as a driver licence number) where it is necessary. They must take reasonable steps to protect unique identifiers from misuse.

NOTE:

The Privacy Act 2020 came into force on 1 December 2020, replacing Privacy Act 1993.

Privacy Act 2020: https://www.privacy.org.nz/privacy-act-2020/privacy-act-2020/

Online Privacy Training: https://www.privacy.org.nz/tools/online-privacy-training-free/