pilchconnect

A specialist legal service for community organisations

Privacy – protecting personal information

Guide for Victorian not-for-profit organisations

Table of Contents

Overview

This Guide is for not-for-profit organisations in Victoria who want to understand more about their obligations under Victorian and Commonwealth privacy legislation.

There are a number of different pieces of legislation (Acts of Parliament) which deal with privacy issues for Victorian community groups. This Guide describes the obligations in the following Acts:

- *Privacy Act 1988* (Cth) which sets out the National Privacy Principles (**Federal NPPs**) and the Information Privacy Principles (**Federal IPPs**)
- *Information Privacy Act 2000* (Vic) which sets out the Information Privacy Principles (**Victorian IPPs**), and
- *Health Records Act 2001* (Vic) which sets out the Health Privacy Principles (**Victorian HPPs**).

Organisations need to consider how they collect, hold, manage, use, disclose or transfer information they hold about individuals, with a view to making sure that they comply with any relevant privacy legislation. And remember that privacy is not just about meeting legal obligations, it can also impact on your organisation's reputation.

Privacy reforms on the horizon:
The Federal Government has recently proposed a series of changes to the *Privacy Act 1988* (Cth). These include new Australian Privacy Principles (APPs) which will contain rules about direct marketing. If these proposals become law then not-for-profit organisations will need to consider how they apply, both generally and to any fundraising activities.

If you would like to keep informed of changes to the law (including any changes to privacy laws), you can sign up to PilchConnect's e-bulletin at www.pilch.org.au/subscribe/.

There are other legal issues that cross over with privacy that are not addressed in this Guide. These include the following areas of law:

- **Confidentiality** – In some circumstances you may have an obligation to keep certain information confidential. This can be because of:
  - an agreement containing confidentiality obligations
  - the commercial or secret nature of the information itself, or
  - the circumstances in which the information was obtained.

PilchConnect has produced some general information on confidentiality laws. Go to Protecting your name, idea and material.

- **Surveillance** - Federal and State laws regulate surveillance, recording, monitoring and interception of communications, including when these are done in the workplace. The laws cover video, audio, computer, telephone and tracking (eg. GPS) surveillance. For information go to the Office of the Australian Information Commissioner.
- **Direct marketing and research** - The *Spam Act 2003* (Cth) regulates how you send promotional emails and other commercial electronic messages, while the *Do Not Call Register Act 2006* (Cth) and related industry standards regulate telemarketing and telephone research. For information go to the Australian Communications and Media Authority (ACMA) and/or the Do Not Call Register website.
- **Freedom of information (FOI)** – If someone has asked to access their information or told you they have a right to it under FOI laws, you will need to consider if that legislation applies to your organisation (eg. if your organisation holds personal information as a result of a contract between it and the government). For information go to the Victorian Government's Freedom of Information online and/or the Australian Government's Office of the Australian Information Commissioner.

Protecting personal information

Commonwealth and Victorian privacy legislation contains a number of sets of rules, called 'privacy principles' which must be followed by an organisation when it is collecting, managing, using and disclosing personal information.

To work out what your organisation needs to do with private information about individuals, follow our four-step approach:

1. What type of information is it?
2. Which privacy principles apply?
3. Does an exemption apply to your organisation?
4. What do the privacy principles require your organisation to do?

We set out the four steps in more detail below.

Note: Even if the privacy principles **don't** apply to your organisation or a particular piece of information that you hold, we recommend that you use them to inform how your organisation collects, uses, stores and discloses information about individuals.

Step 1: What type of information is it?

The privacy principles don't apply to every piece of information your organisation handles.

First, we need to work out if the information you're thinking about falls into one of the categories to which the privacy principles apply – that is, whether it is personal, sensitive and health information.

1. Is it 'personal information'?

The *Privacy Act* (Cth) defines personal information as:

- information, or an opinion (including information or an opinion which is part of a database)
- about an individual,
- whose identity is apparent or can reasonably be ascertained from the information or opinion.

Personal information can be:

- true or false
- verbal, written, photographic or video, and
- recorded or not.

When is 'unrecorded information' personal information?

It can be tricky to work out whether 'unrecorded' information about an individual is subject to the privacy principles. It basically depends on why the information was *collected*.

Personal information that is not collected for the purpose of being included in a 'record' (eg. a document, database or photographic image) is **not** subject to the privacy principles. For example, if a member tells you about what they did on the weekend, but no record is made of that information, then it will be outside the scope of privacy legislation.

However, if the information was collected to be included in a record, and then you communicate that information verbally (for example over the phone), it **will** be subject to the privacy principles.

The *Information Privacy Act* (Vic) includes a similar definition, but it excludes health information because that is covered by the *Health Records Act* (Vic).

'Personal information' **does not** include:

- anonymous information
- aggregated information
- de-personalised information, or
- information about companies or other entities which does not identify individuals.

Tip:
While information about companies will not be covered by privacy laws, it might be covered by confidentiality laws. PilchConnect has produced information confidentiality –see Protecting your name, idea and material on the PilchConnect webportal.

2. Is it 'sensitive information'?

The *Privacy Act* (Cth) defines 'sensitive information' in 3 ways:

1. Personal information or an opinion about an individual's:
    - racial or ethnic origin
    - political opinions
    - membership of a political association
    - religious beliefs or affiliations
    - philosophical beliefs
    - membership of a professional or trade association
    - membership of a trade union
    - sexual preference or practices, or
    - criminal record, or
2. Health information about an individual, or
3. Genetic information about an individual that is not health information.

The *Information Privacy Act* (Vic) includes a similar definition, but it excludes health information because that is covered by the *Health Records Act* (Vic).

3. Is it 'health information'?

'Health information' is a type of personal and sensitive information that is defined broadly under the NPPs and HPPs to include information about mental health, disabilities, health preferences, use of health services, bodily donations and genetics.

4. Does it fall into another special class of information?

These types of information are also covered by privacy laws:

- 'spent convictions' (old, minor criminal convictions)
- tax file numbers
- electoral roll information
- surveillance information, and
- consumer credit history.

We don't cover what you have to do with these kinds of information in this Guide.

Step 2: Which privacy principles apply?

So, you've worked through Step 1 above, and decided that the information you've identified is 'personal', 'sensitive' or 'health' information. Now you need to know which privacy principles you may need to comply with when dealing with that information.

Beware!

Contracts such as funding agreements with government agencies may require you to comply with certain privacy principles. Check your government funding contracts for any privacy obligations.

1. National Privacy Principles (NPPs) - Federal

Your organisation will generally need to comply with the NPPs if it, or a related organisation:

- has an annual turnover over $3 million
- is a health service provider, or
- trades in personal information.

For more information about whether your organisation must comply with the *Privacy Act* (Cth), read the Office of the Australian Information Commissioner's 'Privacy Checklist for Small Business'.

2. Information Privacy Principles (Federal IPPs)

The Federal IPPs apply to Federal and ACT government agencies but may be imposed on your organisation through a contract (eg. a funding agreement with a Federal government department).

3. Information Privacy Principles (Victorian IPPs)

The Victorian IPPs apply to Victorian government agencies, except where the HPPs apply. They may also be imposed on your organisation through a contract (eg. a funding agreement with a Victorian government department).

4. Health Privacy Principles (HPPs) – Victoria

The HPPs apply to Victorian health service providers and, to a lesser degree, to others who handle health information.

Summary table: which set of privacy principles apply?

The below table is a summary only. Please read this in conjunction with the above points, and seek legal advice if you need specific legal help for your organisation.

	Federal NPPs Generally apply to: organisations with turnover of more than $3 million or in other limited circumstances (see above)	**Federal IPPs** May apply to: organisations that have an agreement with the Australian Government (see above)	**Victorian IPPs** May apply to: organisations that have an agreement with the Victorian Government (see above)	**Victorian HPPs** Generally apply to: organisations that are Victorian Health Service Providers or deal with health information in Victoria (see above)
Personal information	✓	✓	✓	☒
Sensitive information	✓	✓	✓	☒
Health information	✓	✓	☒	✓

Step 3: Does an exemption apply?

Once you've worked through which principles may apply, you need to consider if you fall into one of the categories of exemptions. The main categories of exemptions relevant to not-for-profit organisations are addressed below.

Note:
This Guide only provides an overview of the key exemptions. It is important to consider the exemptions carefully because there may be limitations on how they apply. For example, some apply only to the NPPs. Your organisation may need to seek specific legal advice.

1. Employee records

Under the *Privacy Act* (Cth), if an employer does something that is directly related to the employee records of a current or former employee, the employer's conduct is exempt from the NPPs.

This exemption does not apply (and so the NPPs may still apply) if the information is about:

- job applicants
- contractors
- volunteers, or
- employees of related entities.

Remember:
The exemption for employee records only relates to information under the Federal NPPs. The Federal IPPs, and Victorian IPPs and HPPs do not have this exemption.

2. Generally available publications

A publication which is generally available is treated differently to your organisation's own records.

For example, the NPPs will not apply to your copy of the white pages unless you add any of the information from the white pages to your own databases or other records.

3. Government contractors

Government contractors are generally exempt from the NPPs where their conduct is in accordance with a government contract, and that contract is inconsistent with the relevant NPP.

4. Other exemptions

Other exemptions exist but are not usually relevant to community organisations, for example:

- a media exemption – this only applies where an organisation adopts other media privacy standards
- a political exemption, and
- an exemption from some NPPs for transfers of information between related organisations.

For more information about these and other exemptions, go to Office of the Australian Information Commissioner.

Step 4: What do the privacy principles require?

So, your organisation has information about an individual to which the privacy principles apply without an exemption. What do the privacy principles require you to do with that information?

Note:
We have primarily used the NPPs for illustrative purposes in this section of the Guide. In many cases, there will be equivalent principles in the Federal IPPs, HPPs and Vic IPPs.

There are different rules depending on whether you are collecting, using or disclosing, or storing the information. There are also requirements in other circumstances (for example, correcting information) addressed below.

Consent

Tip:
Getting consent can authorise a lot of things that your organisation might want to do with personal information. However it is not always required.

Consent is something that is best to think about 'up front'. It's much easier to get permission from someone when you're collecting their personal information, rather than having to go back to them and ask for it later on. At the outset, therefore, you will need to think about how you're going to use the information that your organisation will collect, so that you can ask for consent.

How do you obtain consent?

Consent does not have to be in writing, but it is a good idea to keep a record of a person's consent in case it is challenged later.

Consent can be express or implied, but privacy regulators:

- caution against relying on 'opt-out' consents
- suggest that consent should be informed (eg. through a privacy notice), and
- suggest that consent should be voluntary.

You need to consider whether an individual has the capacity to give and communicate their consent (eg. are they under 18, or are there questions about mental capacity?). The *Information Privacy Act* (Vic) and the *Health Records Act* (Vic) allow for consent to be given by an authorised representative of the individual, where appropriate.

1. Collection

Collection of personal information

When your organisation is collecting personal information you should:

- only collect information that is **necessary** for what your organisation does
- collect fairly, lawfully and non-intrusively
- collect directly from the individual, if reasonable and practical
- give a privacy notice **(see below)** to the individual
- allow individuals to be anonymous, if appropriate, and
- make sure the person consents before you collect sensitive information (see below for exceptions).

Collection of sensitive and health information

Sensitive information can only be collected in limited circumstances, including:

- where the individual consents
- where the collection is required by law
- under the Vic IPPs only - in some circumstances relating to Victorian Government-funded targeted welfare or educational services
- where the information is collected by a not-for-profit organisation with racial, ethnic, political, religious, philosophical, professional, trade or trade union aims - about active members of the organisation. Note the organisation must have undertaken not to disclose the information without the individual's consent, or
- where the collection is necessary in relation to a legal claim.

Inappropriate use of sensitive information can give rise to discrimination as well as privacy issues. For more information, go to Discrimination and human rights when providing services.

Under the HPPs, there are further limitations on the collection of health information.

Privacy notices

When collecting personal information, NPP 1.3 requires your organisation to take reasonable steps to ensure the individual is aware of:

- your organisation's identity and contact details
- why you are collecting the information
- to whom you usually disclose the information
- any laws requiring the collection
- the individual's rights to access the information from you, and
- the consequences for the individual if your organisation doesn't collect the information.

A common way to meet these requirements is to give an individual a privacy notice when collecting his or her information. Your organisation should consider whether to address other requirements through the privacy notice (eg. obligations to have a privacy policy and obtain the person's consent).

Tips for privacy notices:

- **Don't copy** slabs of text from other websites because the text might:
  - be irrelevant to your organisation's collection, use or disclosure of the information
  - be drafted according to laws from different States or countries
  - not cover all of the requirements in NPP 1.3, or
  - be protected by copyright.
- **Don't over commit**. An example of promising too much could be: 'we will never disclose your information without your consent'.
- **Keep updated**. Specific website security technologies can be used to protect information and these technologies update regularly.

2. Use and disclosure

Personal, sensitive and health information can be used and disclosed by an organisation when the use or disclosure:

- is for the main purpose for which the information was collected

- is for other related purposes for which the individual would reasonably expect the information was collected
- is made with the specific consent of the individual
- is required in an emergency
- is required or authorised by law
- is for the purposes of law enforcement
- is required because there is suspected fraud or unlawful activity, or
- is required for some types of research that are in the public interest.

There are some additional permitted uses and disclosures in relation to health information under the NPPs and HPPs.

Transferring information overseas or interstate

NPP 9 limits an organisation's ability to transfer information about an individual to others outside Australia. Vic IPP 9 and HPP 9 impose similar limitations on the transfer of personal or health information to third parties outside Victoria.

Generally transfers of information are allowed if:

- there is consent by the person who's information it is, or
- there are appropriate contractual restrictions on the third party who is receiving the information.

There are some other exceptions to the limitations. You should seek specific legal advice if required.

3. Storage

Storage obligations when holding information

Your organisation must take reasonable steps to protect the security of personal, sensitive and health information that it stores.

When the information is no longer required, organisations must destroy or de-identify personal information, except in the case of health information which is held by a health service provider. Health information of that type must be retained in accordance with HPPs 4.2 – 4.4.

Security measures

Your organisation should consider what sort of information it holds and how best to meet its obligations regarding security of the information.

Depending on your organisation's circumstances, you should consider the following security measures:

- requiring staff to keep relevant documents in locked drawers or cabinets
- placing access restrictions on relevant documents or systems including electronic access restrictions
- enforcing a 'clean desk' policy to minimise the risk of inadvertent disclosure of personal information
- placing computer screens out of the view of others, particularly visitors to the organisation
- limiting the use of portable storage devices, including laptops, disks and USB keys or using encryption or other security measures
- recording audit trails of access to documents
- encrypting documents containing personal information, particularly when those documents are being sent by email
- including email addresses for group emails in the 'BCC' field rather than the 'To' field so recipients cannot see other recipients' email addresses
- including confidentiality and privacy clauses in agreements with volunteers or others who have access to the personal information, and
- making sure employees, volunteers or others return information at the end of their employment or relevant involvement with the organisation.

Accessing personal information

The *Privacy Act* (Cth), the *Information Privacy Act* (Vic) and the *Health Records Act* (Vic) all set out circumstances under which organisations must allow individuals to access and, if necessary, correct their personal information.

Tip:
Make it a policy of your organisation not to record inappropriate information about individuals.

There are a number of exceptions to the access requirements.

Organisations can charge a fee for providing access to personal information, but the charges must:

- be notified in advance
- not be excessive, and
- not apply to making a request for access.

Organisations can refuse to provide access until the fee is paid.

The Victorian laws require access to be provided within 45 days, while the Privacy Commissioner recommends that access under the Commonwealth laws is provided within 30 days. Reasons must be given if an organisation refuses to give access.

Remember:

- We don't go into the detail in this Guide about when individuals can access information about themselves from your organisation. This is because the law is quite specific and lots of organisations are exempt in some way or another.
- It's a complicated area, and you might need legal advice if accessing information is becoming a hot topic for your organisation.

4. Other requirements

- **Data quality**: Your organisation must take reasonable steps to ensure that the personal information your organisation collects, uses, discloses and stores is accurate, complete and up-to-date.
- **Government identifiers**: There are requirements to limit the use and disclosure of government identifiers (eg. Medicare number).
- **Correcting personal information:** If an individual can show that the information about him or her that an organisation holds is inaccurate, incomplete or out-of-date, the organisation must:
    - take reasonable steps to correct the information, or
    - if there is disagreement about the accuracy, attach a statement noting that the individual claims the information is incorrect, incomplete and out-of-date.

  Health information must not be deleted when it is being corrected, other than in accordance with HPP 4.2.

  Vic IPP 6.8 requires corrections to be made, or an explanation of why the organisation refuses to make the correction, within 45 days of the request. HPP 6.9 requires a decision about a request to correct health information to be notified to the individual within 30 days of the request.

Enforcement and/or penalties

NPPs/IPPs (Federal)

Under the *Privacy Act* (Cth), the Privacy Commissioner can make orders, including orders for compensation and remedial actions.

HPPs/IPPs (Vic)

Under the *Information Privacy Act (Vic)* and the *Health Records Act* (Vic), the Victorian Privacy Commissioner can investigate and conciliate complaints, and also refer a complaint to VCAT. VCAT can make an order about whether a person's privacy has been breached and order a person or organisation to pay compensation up to $100,000.

Resources

Legislation

Privacy Act 1988 (Cth)
Information Privacy Act 2000 (Vic)
Health Records Act 2001 (Vic)

Victoria

- Privacy Victoria

  This website provides information about the Victorian IPPs, including an information sheet on exemptions from the *Information Privacy Act*.

- Office of the Health Services Commissioner

  This website provides information about the Victorian HPPs.

Commonwealth

- Office of the Australian Information Commissioner

  This website provides information about NPPs/Federal IPPs, including information sheet coverage of and exemptions from the Private Sector Provisions.

- Australian Communications and Media Authority (ACMA)

  ACMA is responsible for regulating online content (including internet and mobile content) and enforcing Australia's anti-spam law. This website provides information on the Do Not Call Register.